



**HVDC-WISE**

# Protection Concepts for AC/DC architectures

## **D3.3: Protection Concepts**

## Document Properties

Funding Program	Horizon Europe and UK Horizon Europe funding guarantee	
Grant Agreement Number	101075424 (UK 10041877 and 10051113)	
Project	HVDC-WISE	
Deliverable Id	D3.3	
Title	D3.3: Protection Concepts	
Distribution Level	Public	
Due Date	May 2024	
Date Submitted	September 2024	
Status	Reviewed version	
Version	2	
Work package / Task	3.3	
Authors	PEREZ, Filipe	SGI
	CASTELLANOS, Jesús	SGI
	ANHAUS, Sarah	RWTH
	PRESEKAL, Alfán	TU Delft
	JORJANI, Mohsen	TU Delft
	STEFANOV, Alex	TU Delft
Contributors	XU, Lie	Strathclyde University
Acknowledgement	LETERME, Willem	RWTH
	MCGUINNESS, Sean	EPRI
	CIRIO, Diego	RSE

## Version History

Version	Date	Comment
1	31/05/2024	First submitted version
2	21/10/2024	Final version

## Approval Flow

Title	Person	Date	Comment
Task Lead	Filipe Perez	21/10/2024	Approved
WP Lead	Robert Dimitrovski	21/10/2024	Approved
Coordinator	Juan Carlos Gonzalez	21/10/2024	Approved

Copyright © HVDC-WISE, all rights reserved. This document may not be copied, reproduced, or modified in whole or in part for any purpose. In addition, an acknowledgement of the authors of the document and all applicable portions of the copyright notice must be clearly referenced. Changes in this document will be notified and approved.



HVDC-WISE is supported by the European Union's Horizon Europe program under agreement 101075424.

UK Research and Innovation (UKRI) funding for HVDC-WISE is provided under the UK government's Horizon Europe funding guarantee [grant numbers 10041877 and 10051113].

### D3.3: Protection Concepts

Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union or European Climate, Infrastructure and Environment Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

# Table of Contents

<b>Executive Summary</b>	<b>11</b>
<b>1. General Introduction</b>	<b>13</b>
1.1. DC Protection	13
1.2. AC Protection	15
1.3. Cyber Security	16
<b>2. DC Fault-Ride Through Analysis</b>	<b>18</b>
2.1. Strong Grid Scenario	27
2.2. Weak Grid Scenario	33
2.2.1. GFM Control Implementation	36
2.2.2. Operational limits (Current limitation)	49
2.3. Including Frequency Dynamics in the AC Grid	55
2.3.1. Oversizing the converters	59
2.3.2. Energy Storage Insertion	62
2.3.3. Frequency dynamics interaction (VSM and SG)	64
2.3.4. Local RoCoF Index	67
2.4. Power Electronic Grid Scenario	70
2.4.1. DC Fault (pole to ground)	72
2.4.2. Oversizing the Converters	79
2.4.3. Energy Storage Insertion	82
2.5. Fully Selective philosophy	84
2.5.1. Pole-to-pole fault	87
<b>3. AC Protection Impacts</b>	<b>91</b>
3.1. Differentiating between protection concepts	91
3.2. Distance Protection Relay	92
3.2.1. Functionality	95
3.2.2. Consideration of distance protection in the presence of converters	97
3.3. Investigating Protection Relay Behavior Using a Simplified Test Network	101
3.3.1. GFL control	103
3.3.2. GFM Control	103
3.3.3. Test Studies	105
<b>4. Cyber Security Events</b>	<b>122</b>
4.1. Cyber-Physical HVDC System	122
4.2. Cyber Threats and Vulnerabilities on HVDC	124
4.2.1. False Data Injection Attacks	124
4.2.2. Replay and Spoofing Attacks	125
4.2.3. Denial of Service	127
4.3. Cyber-Physical HVDC Co-Simulation	127
4.3.1. State-of-the-Art HVDC Model and Co-Simulation	128
4.3.2. Cyber-Physical HVDC Model and Co-Simulation	129

## D3.3: Protection Concepts

4.3.3.	Cyber Threat Model	131
4.3.4.	Cyber Attack Impact Assessment	132
4.4.	<i>HVDC Cyber Attack Mitigation</i>	135
4.4.1.	State-of-the-Art Cyber Attack Mitigation on HVDC	135
4.4.2.	Deep Learning for Throughput Anomaly Detection	139
4.4.3.	Forensic Graph Model for Anomaly Localization	143
4.4.4.	Implementation of Secure Standard Protocol	146
<b>5.</b>	<b>General Conclusions</b>	<b>148</b>
5.1.	<i>DC FRT Analysis Conclusions</i>	148
5.1.1.	Characterization of DC-FRT	149
5.1.2.	Recommendations for DC-FRT in GFM converters	150
5.1.3.	Current limitation issues	151
5.1.4.	Influence of frequency dynamics in DC faults	152
5.1.5.	Possibilities of energy resource allocation	152
5.1.6.	Issues in PE based grids	153
	<i>AC Protection Impacts Conclusions</i>	154
	Recommendation	155
5.2.	<i>Cyber Security Events Conclusions</i>	156
	<b>Bibliography</b>	<b>158</b>

# List of Figures

Figure 2-1: Generic electrical model of the studied system: AC grid connected into the meshed MTDC grid.	23
Figure 2-2: The bipolar configuration of the MTDC meshed grid.	23
Figure 2-3: Protection coordination sequence.	24
Figure 2-4: General control structure of the MMC in GFL.	26
Figure 2-5: General control structure of the MMC in GFM.	27
Figure 2-6: Electrical model of strong grid connected to the meshed MTDC grid.	28
Figure 2-7: DC voltage and DC current of Station 1 in pu, negative pole in red and positive pole in blue.	29
Figure 2-8: Active Power profile in Pos_S1 and Neg_S1, and their references.	30
Figure 2-9: Reactive power profile in Pos_S1 and Neg_S1, and their references.	30
Figure 2-10: AC voltage on the PCC.	31
Figure 2-11: Active power in the stations of the meshed DC grid.	32
Figure 2-12: Reactive power in the stations of the meshed DC grid.	32
Figure 2-13: Electrical model of strong grid connected to the meshed MTDC grid.	33
Figure 2-14: Comparison of active power profile between strong and weak grid.	34
Figure 2-15: Comparison of reactive power profile between strong and weak grid.	35
Figure 2-16: AC voltage magnitude at the PCC, strong and weak grid comparison.	35
Figure 2-17: DC voltage at the positive and negative poles, strong and weak grid comparison.	36
Figure 2-18: Total energy in the faulty pole (Pos_S1).	36
Figure 2-19: Adjusted time-scale protection sequence for GFM control.	38
Figure 2-20: Active power profile of station S1 in GFM control.	39
Figure 2-21: Reactive power profile of station S1 in GFM control.	40
Figure 2-22: The AC voltage magnitude at the PCC.	40
Figure 2-23: the AC voltage magnitude and three-phase waveform zoom during fault transient.	40
Figure 2-24: DC voltage at the positive and negative poles.	41
Figure 2-25: internal energy of the positive pole in station 1.	42
Figure 2-26: Active Power profile in station 1, considering GFM to GFL proposal.	43
Figure 2-27: Reactive Power profile in station 1, considering GFM to GFL proposal.	44
Figure 2-28: DC voltage in station 1, considering GFM to GFL proposal.	44
Figure 2-29: AC voltage magnitude in the PCC, considering GFM to GFL proposal.	45
Figure 2-30: Positive pole converter total energy.	45
Figure 2-31: Block diagram of the outer energy control loop.	46
Figure 2-32: Active power profile in station 1, considering GFM with outer energy control proposal.	47
Figure 2-33: Reactive power profile in Station 1, considering GFM with outer energy control proposal.	48
Figure 2-34: DC voltage at the positive and negative poles.	49
Figure 2-35: The AC voltage magnitude at the PCC.	49
Figure 2-36: Positive pole converter total energy.	49
Figure 2-37: Active power profile in station 1, considering CSA approach.	52
Figure 2-38: Id and Iq currents considering the reference limits for CSA approach.	52
Figure 2-39: Active Power profile in station 1 for VI approach.	53
Figure 2-40: Id and Iq currents (top), AC current magnitude and maximum limit (bottom) for VI approach.	54

Figure 2-41: Active power profile in station 1 considering the deblocking of the MMC simultaneously with the reclose of the DCCB.	55
Figure 2-42: Internal energy of the faulty pole when the deblocking of the MMC occurs simultaneously with the reclose of the DCCB.	55
Figure 2-43: Electrical model of synchronous machine connected to the MTDC meshed grid.	56
Figure 2-44: Active Power profile in station 1 connected with a synchronous machine.	57
Figure 2-45: Frequency dynamics of the system considering Station 1, synchronous machine and the PLL measurement.	58
Figure 2-46: Reactive power profile in station 1 connected to a synchronous machine.	58
Figure 2-47: The AC voltage magnitude at the PCC when the synchronous machine is connected.	59
Figure 2-48: Active power profile in Station 1 connected with a synchronous machine.	60
Figure 2-49: Zoom in the active power profile in Station 1 connected with a synchronous machine.	60
Figure 2-50: Frequency dynamics of the system considering Station 1, synchronous machine and the PLL measurement.	61
Figure 2-51: The AC voltage magnitude at the PCC when the synchronous machine is connected.	61
Figure 2-52: Reactive Power profile in station 1 connected to a synchronous machine.	62
Figure 2-53: Energy storage active power reference profile.	62
Figure 2-54: Active power profile in station 1 connected with a synchronous machine.	63
Figure 2-55: Frequency dynamics of the PLL measurement at the PCC and the synchronous machine.	64
Figure 2-56: Active Power profile in station 1 connected with a synchronous machine, when considering the load shift.	65
Figure 2-57: Internal Energy of the positive and negative converters from station S1.	66
Figure 2-58: VSM frequency of the converters in station S1.	66
Figure 2-59: Frequency dynamics of the synchronous machine.	66
Figure 2-60: The AC voltage magnitude at the PCC connected the synchronous machine, when considering the load shift.	67
Figure 2-61: AC grid composed of synchronous machine and bulk system (COI) connected to station S1.	68
Figure 2-62: Active power and frequency considering the SG and the bulk system.	69
Figure 2-63: Frequency variation for the SG and the bulk system in case A.	70
Figure 2-64: Zoom in the SG and bulk system frequency to better understand the RoCoF variation in both systems.	70
Figure 2-65: Electrical model of the PE grid (GFM+GFL) connected to the meshed MTDC grid.	72
Figure 2-66: Active power profile in PE_GFM, PE_GFL, POS_s1 and neg_s1, and their references.	74
Figure 2-67: Zoom in the active power profile in PE_GFM, POS_s1 and neg_s1, and their references.	75
Figure 2-68: Current magnitude in Pos_S1, Neg_S1 and PE_GFM converters.	76
Figure 2-69: VSM frequency dynamics in PE_GFM, Pos_s1 and Neg_s1.	76
Figure 2-70: Reactive power profile in the PE grid.	77
Figure 2-71: Ac voltage magnitude at the PCC considering the PE grid.	78
Figure 2-72: Zoom in the AC voltage magnitude and three-phase waveform during fault transient.	78
Figure 2-73: DC voltage positive and negative poles of station S1 considering the PE grid.	79
Figure 2-74: Active power profile in PE_GFM, PE_GFL, POS_s1 and neg_s1, and their references.	80
Figure 2-75: VSM Frequency dynamics in PE_GFM, Pos_s1 and Neg_s1, and the measured PLL frequency.	81
Figure 2-76: Reactive power in AC side of the grid and the voltage profile in the PCC.	81
Figure 2-77: DC voltage positive and negative poles.	82

Figure 2-78: Power dispatch profile of the storage in the AC grid.	83
Figure 2-79: Active power profile considering the AC energy storage.	83
Figure 2-80: VSM frequency of the PE grid considering the AC energy storage.	84
Figure 2-81: AC voltage on the pcc considering the AC energy storage.	84
Figure 2-82: Electrical model of the MTDC with FS protection philosophy.	85
Figure 2-83: Active power profile of Station 1 and the respective measured frequency, considering FS philosophy.	86
Figure 2-84: Reactive power profile of Station 1 and the AC voltage on the PCC, considering FS philosophy.	87
Figure 2-85: DC voltage on the positive pole, considering FS philosophy.	87
Figure 2-86: Active power profile of Station 1 and the respective measured frequency, in pole-to-pole fault.	88
Figure 2-87: Reactive power profile of Station 1 and the AC voltage on the PCC, in pole-to-pole fault.	89
Figure 2-88: DC voltage on the Station 1 in pole-to-pole fault.	90
Figure 3-1: Example of graded distance protection zones.	93
Figure 3-2: Relay Characteristics (Protection zones- Main and backup)	94
Figure 3-3: Measured fault-loop impedances during a phase-to-ground fault.	94
Figure 3-4: IEC 60255-121:2014 standard for distance protection relay	95
Figure 3-5: Modified nine-bus AC network model, implemented in PSCAD based on [53], [54].	102
Figure 3-6: Current control loop.	103
Figure 3-7: Power control loop.	103
Figure 3-8: P-f droop (above) and Q-V droop (below) implementations.	104
Figure 3-9: Voltage control loop.	104
Figure 3-10: Test cases considering different infeed source variations.	105
Figure 3-11: Movement of a measured loop-impedance from pre-fault to post-fault conditions (86km)	106
Figure 12: Current Curves for various combinations: Ideal Source, SG and SG, GFL and GFL, GFM and GFM, GFM and GFL (86km)	107
Figure 13: Voltage Curves for various combinations: Ideal Source, SG and SG, GFL and GFL, GFM and GFM, GFM and GFL (86km)	108
Figure 14: Current Curves for various combinations: Ideal Source, SG and SG, GFL and GFL, GFM and GFM, GFM and GFL (20km)	108
Figure 15: Voltage Curves for various combinations: Ideal Source, SG and SG, GFL and GFL, GFM and GFM, GFM and GFL (20km)	109
Figure 16: Current Magnitudes after the FFT for various combinations: Ideal Source, SG and SG, GFL and GFL, GFM and GFM, GFM and GFL (86km)	109
Figure 17: Voltage Magnitudes after the FFT for various combinations: Ideal Source, SG and SG, GFL and GFL, GFM and GFM, GFM and GFL (86km)	110
Figure 18: Current Magnitudes after the FFT for various combinations: Ideal Source, SG and SG, GFL and GFL, GFM and GFM, GFM and GFL (20km)	110
Figure 19: voltage Magnitudes after the FFT for various combinations: Ideal Source, SG and SG, GFL and GFL, GFM and GFM, GFM and GFL (20km)	111
Figure 3-20: Variations in the controller bandwidth (86 km line)	112
Figure 3-21: Variations in the controller bandwidth (20 km line)	113
Figure 3-22: Fault-loop resistance between two GFMs.	113
Figure 3-23: Variations in the controller bandwidth (86 km line).	114
Figure 3-24: Variations in the current limits (86 km line).	115

Figure 3-25: Variations of the current limits (20 km line).	115
Figure 3-26: Variations of the current limits, sampled 40 ms later (86 km line).	116
Figure 3-27: Variations of the current limits, sampled 40 ms later (20 km line).	116
Figure 3-28: Fault-loop resistance between two GFMs (current limit variations).	117
Figure 3-29: Fault-loop resistance between two GFLs (current limit variations).	117
Figure 3-30: Fault-loop resistance between A GFM and a GFL (current limit variations).	118
Figure 3-31: Comparison between current saturation limiting (CSL) and virtual impedance (VI) in two GFMs.	119
Figure 4-1: HVDC Cyber-physical system.	123
Figure 4-2: STRUCTURE OF GOOSE DATA FRAME	127
Figure 4-3: Comparison of normal and spoofed goose frame.	127
Figure 4-4: HVDC System Model four-terminal terminal MMC-based MTDC network.	130
Figure 4-5: HVDC System Model Implementation on RTDS.	130
Figure 4-6: Hardware In the loop (HIL) Setup.	131
Figure 4-7: HVDC system under normal operations.	132
Figure 4-8: Wind turbine (AC) line fault.	133
Figure 4-9: HVDC line fault.	133
Figure 4-10: Goose Attack on Wind turbine circuit breaker.	134
Figure 4-11: Goose Attack on MMC circuit breaker.	134
Figure 4-12: traffic comparison from different scenarios.	135
Figure 4-13: Cyber kill chain stages and Impacts.	140
Figure 4-14: Forensic graph model for anomaly detection.	141
Figure 4-15: Statistical comparison between normal, predicted, and attack or anomalous traffic for data A, B, and C.	145
Figure 4-16: ROC comparison for data A, B, and C.	145
Figure 4-17: Forensic graph model plots.	146

# List of Tables

Table 1-1: List of participants of Task 3.3 and the activities description.	12
Table 2-1: AC system criteria according to the fault probability.	18
Table 2-2: The selected case scenarios.	21
Table 2-3: Initial power flow in the MTDC.	24
Table 2-4: Initial power flow in AC grid.	24
Table 2-5: MMC parameters in all stations.	25
Table 2-6: MMC blocking parameters.	25
Table 2-7: Initial power flow in Station 1 when operating close to the power limits.	51
Table 2-8: Initial Power flow in the MTDC when station 1 is close to power limits.	51
Table 2-9: Electrical parameter of the synchronous machine.	56
Table 2-10: Comparison of local RoCoF for COI and SG in 3 different cases.	68
Table 2-11: Initial power flow in AC grid for the PE grid.	72
Table 2-12: Initial power flow in the MTDC for the PE grid.	72
Table 2-13: Initial power flow in AC grid for the PE grid.	79
Table 3-1: Differences between SGs and Converters Short Circuits [52]	99
Table 3-2: Comparison between different infeed sources.	100
Table 3-3: Influencing factors on the distance protection relay.	119
Table 4-1: Survey on cyber-attacks targeting HVDC systems components.	124
Table 4-2: Survey on HVDC co-simulation.	128
Table 4-3: Simulated scenarios.	132
Table 4-4: Summary of cyber defense methods in HVDC power grids.	135
Table 4-5: Summary of Network Traffic Data.	144
Table 5-2: Vulnerabilities for different topologies in terms of AC protection.	155

# Executive Summary

The integration of High Voltage Direct Current (HVDC) systems into modern power grids presents a promising path for enhancing grid resilience and efficiency. However, ensuring the reliable operation of HVDC-based grid architectures among various fault scenarios remains a critical challenge. Task 3.3 of HVDC-wise project focuses on developing guidelines for the cost-effective design of HVDC-based grid architectures' protection systems, enabling them to withstand faults occurring on the DC side, the AC side, or within the cyber-layer. These guidelines are essential for the design and implementation of realistic use cases in WP6 and WP7.

Subtask 3.3.1 is focused on the protection of the DC side, aiming to design AC/DC systems capable of surviving DC faults while considering their broader impacts on the entire AC/DC transmission system. Through extensive Electromagnetic Transient (EMT) simulations and analysis, various protection schemes are evaluated to understand their effects on AC grid stability, grid inertia, and converter control modes. Subsequent phases will focus on devising dedicated HVDC control strategies to mitigate these impacts effectively.

Subtask 3.3.2 delves into the protection of the AC side, emphasizing the analysis of AC protection in converter-dominated areas. The primary objective is to assess how protection relays will be affected due to control concepts and grid specifications to assess impacts and derive future requirements of current AC line protection. By defining simulation scenarios and evaluating different fault scenarios, this subtask aims to provide guidelines on AC protection philosophies in coordination with control strategies and grid specifications.

Subtask 3.3.3 addresses the protection of the cyber layer, investigating vulnerabilities and impacts of cyber-attacks on HVDC systems. Moving beyond traditional High Voltage Alternating Current (HVAC) system security, this subtask aims to qualitatively assess the inclusion of communication-related aspects in assessing cyber-resilience. By studying sophisticated cyber-attacks and modelling communication network protocols, this subtask seeks to identify reliable anomaly detection methods for HVDC-HVAC cyber-physical systems.

With SGI, RWTH, and TUD leading the respective subtasks and contributions from various industry partners and academic institutions, Task 3.3 embodies a collaborative effort to develop robust protection strategies for HVDC-based grid architectures, ensuring their resilience in the face of evolving grid conditions and cyber threats. These strategies will play a crucial role in shaping the future of power grid infrastructure, facilitating sustainable and reliable energy transmission.

This document is organized as follows: a general introduction regarding HVDC protection, relating AC and DC side and cyber-attacks is provided in chapter 1. The DC FRT analysis from Subtask 3.3.1 is introduced in chapter 2. Subtask 3.3.2 referring to the AC protection impacts is introduced in chapter 3 and contributions of cyber security events are done in chapter 4. The conclusions and recommendations for the next working packages are detailed in chapter 5 and at last, the bibliography is provided.

The organization of Task 3.3 regarding the participants, leaders of the subtasks and the description of the task activities are summarized in Table 1-1.

**TABLE 1-1: LIST OF PARTICIPANTS OF TASK 3.3 AND THE ACTIVITIES DESCRIPTION.**

PARTICIPANTS	DETAILS OF PARTICIPATION
<b>Lead:</b> SGI <b>Contributors:</b> RWTH, UOS, AMP, TTG, SSE	<b>Subtask 3.3.1 – Protection of the DC side</b> - Analysis on how the DC faults and protection actions impact AC stability aspects - Analysis of protection actions coordinated with control strategies in case of DC fault occurrence
<b>Lead:</b> RWTH <b>Contributors:</b> AMP, TTG, SSE	<b>Subtask 3.3.2 – Protection of the AC side</b> - Identification of the impact of future grid conditions on AC protection - Evaluation of requirements for the existing protection philosophy
<b>Lead:</b> TUD <b>Contributors:</b> SSE	<b>Subtask 3.3.3 – Protection of the cyber layer</b> - Study of sophisticated cyber-attacks of the AC/DC system architectures - Modelling communication network protocols

# 1. General Introduction

The Multi-Terminal High Voltage Direct Current (MTDC) grid is the next step for High Voltage Direct Current (HVDC) transmission, allowing power to be exchanged between multiple geographically distant points, emerging as a possible solution for the integration of large-scale renewables as Offshore Wind Farms (OWF) and the interconnection multiple AC areas without the need of synchronization. Therefore, the benefits of MTDC grids include the capacity to share and balance power reserves, reduce the overload of AC areas while improving the system operation by providing ancillary services. However, the expansion of HVDC systems and their integration into the existing AC system poses significant challenges for modern power grid operation and protection.

A lot of effort has been put into ensuring the reliability and resiliency of MTDC grids, where several control and protection methods have been proposed to assure the proper operation and security of such AC/DC systems. Nevertheless, there are control and protection challenges to achieve the desired reliability and resilience feature of future network:

- **Protection in case of DC fault:** Protection during DC faults is crucial for maintaining the reliability of MTDC grids. Various technologies, such as DC circuit breakers, AC circuit breakers, and fault-current-capable converters, have been explored. However, integrating these technologies and coordinating them with other MTDC components requires thorough investigation to establish standardized protection strategies.
- **Operation and control:** Safe operation of MTDC grids refers to maintaining the stability of DC voltage inside of the operational limits. Therefore, converters control target is to keep the DC voltage controlled according to grid requirements, damping the disturbances from both AC and DC side of the grid. This performance relies on the proposed control strategy for the converter, on the other hand the converter topology and the system parameters have also an influence on the system behavior. Despite numerous studies, additional exploration is necessary. Additionally, the interoperability challenge arising from components sourced from various manufacturers within the MTDC grid must be tackled.
- **Interaction with the AC system:** numerous studies on modeling and controlling MTDC systems overlook the dynamics of AC systems by simplifying it as an infinite bus. Understanding potential interactions requires comprehensive analysis of the hybrid AC/DC system.

To bring solutions within the context of the expansion of HVDC systems in transmission systems aimed at improving system reliability and resilience, this report focuses on the investigation of the AC and DC protection of AC/DC systems and the vulnerability of the protection schemes with respect to the cyber-security. Therefore, the preliminary protection solutions and recommendations are going to be provided considering the impacts of AC and DC faults regarding to different control strategies and different AC/DC grid configurations foreseen in the future network expansion. They will give the possibility to propose indexes to pave the way for deriving DC grid planning standards. The analysis includes the identification of security issues for the proposed protection strategies and how they impact the system operation when considering different control strategies.

## 1.1. DC Protection

In the context of DC protection, the HVDC-wise project aims to understand and foresee the possible impacts of DC-side protection on the AC/DC system dynamics. Therefore, the initial studies of DC protection behavior and impacts on MTDC systems will be conducted in Chapter 2 of this report, regarding the protection philosophies with major impacts to the system stability and operation.

DC protection can be considered as a recent solution for ensuring the safety of HVDC networks during DC fault in the development of MTDC networks. The DC protection challenge persisted until various methods for DC fault isolation were proposed. The main problem in DC fault protection arises from the complexity of interrupting fault currents, due to the absence of zero crossing in the current waveform and the limited overcurrent handling capacity of converters [1].

Initially, the most common approach for point-to-point HVDC links is the use of AC circuit breakers (ACCBs) where a DC-side fault implies the loss of the entire interconnection. Therefore, alternative approaches to DC fault current interruption have been explored: integrating DC circuit breakers (DCCBs) into the DC network and using converters equipped with fault blocking features (e.g. full bridge MMC). DC protection strategy involves coordinating protection equipment and devices in the grid to perform the follow operation in coordination:

1. Detect a DC fault
2. Interrupt DC fault currents
3. Isolate affected cables/lines
4. Restore stable system operation

Industry and academia have worked on various protection strategies, but finding the best one to use is still a research challenge. Understanding how these strategies affect the AC grid will help to choose the best strategy [2].

As the technology evolves, the use of more complex converter station configurations, e.g., bipoles, and the consideration of larger DC topologies, such as radial arrangements or meshed networks, pushed DC protection power system engineers to include different levels of selectivity, since the permanent and temporary loss of the whole DC system would imply the disconnection of critical loads and power sources in an AC/DC system. Therefore, three main philosophies have been proposed in the recent years based on a level of selectivity: fully selective, non-selective and partially selective philosophies [3, 4], they as described as follows:

- **Fully selective** philosophy: protection zones are defined to have isolation solely of the faulted element, i.e., a line, cable, busbar, or converter (each element is considered a protection zone).
- **Non-selective** philosophy: it isolates the complete DC system in case of an event on the DC side (only one protection zone for the whole DC grid).
- **Partially selective** philosophy: the DC system is divided into several protection zones, based on particular considerations, allowing the isolation of a section of the system and the further operation of the others.

These philosophies might be implemented by means of specific protection strategies considering different elements, such as switching stations containing DC circuit breakers (DCCBs), fast switches, line inductors, residual current breakers, among other protection equipment that will enable the proper functioning of each of those strategies. Furthermore, these strategies require sufficient measuring devices and proper sampling to react in the stringent periods required to maintain a secure operation of the hybrid system.

A methodology to design the DC protection system is proposed in [5] taking into consideration the NSWPH project. The study aims to optimize the DC protection components and busbar topologies to ensure reliable and cost-effective operation of the OWF transmission system. The main aspects are summarized next:

- Fully selective fault clearing strategies are deemed feasible for the study case, while non-selective fault clearing strategies do not meet AC system criteria due to Temporary Stop (TS) limits.
- Partially selective strategies or a combination of different protection strategies could be viable with slight relaxation of AC system criteria.
- For nodes with 2 GW or less, the Double Busbar Single Breaker (DBSB) configuration is recommended, allowing omission of the DC breaker at the MMC Wind Farm output.
- For nodes with 3 GW or more, the One Breaker and a Half (OBH) configuration is recommended for optimal protection.
- Hybrid DC breakers and Mechanical DC breakers are identified as feasible solutions, with cost considerations favoring the former in terms of CAPEX.
- The installation of large DC series reactors can impact the dynamics of the DC grid and may lead to stability issues, necessitating further research on DC reactor design criteria for system stability enhancement.

Future enhancements in control solutions and a deeper understanding of temporary power stop based on interconnected AC zones could optimize protection strategies, busbars, and protection components. These conclusions highlight the importance of selecting appropriate protection strategies and components to ensure the reliability, stability, and cost-effectiveness of the DC grid in offshore wind energy transmission systems like the NSWPH project.

The DC protection design has impacts on the system stability, costs, and even determining temporary and permanent stops that affect the energy non-served, which results to be a critical aspect for the expansion of MTDC grids. The dynamic behavior of the systems relies on the interaction between the control strategies with the selected protection philosophies and the grid configuration. Therefore, it is important to understand the behavior of protection considering different control strategies and how they affect the operation and stability of the system.

This study delves into understanding DC contingency events and their impact on AC/DC system architecture, emphasizing fundamental aspects of DC faults and their repercussions on the AC side. The effectiveness of protection strategies and control actions hinges on system architecture and coordination. As future power systems integrate AC/DC configurations, each poses distinct stability concerns, necessitating a comprehensive review of hybrid system DC fault-ride through (FRT) mechanisms, encompassing control and protection implementation, and scrutinizing AC side impacts.

## 1.2. AC Protection

Through the increase of converters and the reduction of conventional power plants within the network, inertia will decrease in the future. These advanced power-electronic systems behave differently from traditional generators when they face short circuit faults especially in terms of initial transients, lower short-circuit power, and lower inertia. Specifically, the current-carrying capability of converters has a major impact on cost, so the current limit tends to be limited to some value just marginally greater than nominal converter current. The phase angles of the converter current during faults are influenced by the design of the converter controller [6]. Protection systems in transmission networks are designed based on the transient and steady-state characteristics of grids powered by synchronous generators and decades of experience with transient disturbances and asset failures [7]. When a fault occurs within the system, these generators immediately supply a large current. Protection relays can detect faults as the fault current magnitude is usually many times larger than

the current under normal grid conditions. Grid assets are designed to carry these fault currents without damage or failure for a short period of time. For example, AC circuit breakers and associated busbar conductors and structures are designed to stop fault currents as high as 63 kA [8].

The difference in fault current characteristic between synchronous-generators and converters can create challenges for certain protective systems. For example, the reliability and security of distance protection algorithms used to protect AC transmission lines, especially for those near converters, can be impacted under certain conditions [9]. Transmission grid owners and operators have experienced a number of issues with distance protection algorithm response to short circuit fault near converters. These events tend to be isolated and constitute a small proportion of overall protection failures in any given year. Furthermore, they can often be rectified by revising protection settings methodologies, although in certain cases relay hardware upgrades or a change to Protection and Control Philosophies have been found necessary. These problems include, but are not limited to, underreaching or overreaching of distance protection zones, erroneous identification of faulted phase(s) or fault direction, and other forms of algorithm-specific malfunction. Due to this approach, the following questions may arise:

1. *How do the distinctive fault current behaviors of existing converter designs, such as limited magnitude and phase angle variations influenced by control mechanisms, challenge the existing distance protection schemes and the reliability of protective systems?*
2. *What comprehensive strategies can be applied to address inaccuracies in zone selection and fault direction identification in distance protection schemes, considering the interplay between grid specifications, operational conditions, and protection relay functionalities?*

This highlights the need for a comprehensive understanding of how grid specifications and environmental conditions impact the performance of distance protection relays. The primary objective of this research is to examine the effects of different AC grid characteristics by varying different grid strength levels and infeed sources in an IEEE 9 node network on the distance protection. By first varying the short-circuit power of a grid serves a simplified representation of various grid scenarios with weak grids, which will arise by the extensive integration of converters. The variation of grid strength is necessary since they may vary in the future – depending proportional of the synchronous and converter infeed. As a reference the starting point of the study will be a grid with a higher short-circuit power. By varying the infeed sources in a network and exploring control concepts like grid-following and grid-forming can demonstrate their effects on the performance of protection relays.

Within this work package, several test scenarios confirm the concern about the reliability of the distance protection relay, which should be investigated more in-depth in work package 7. The research concentrates on distance protection, specifically on the zone element (R-X-coordinates). It allows to identify impedance shifts within the coordination system and if the fault impedance will shift between two impedance zones. This can indicate a potential for inadequate impedance detection. The investigation emphasizes how different short-circuit powers / infeed sources can influence impedance zone detection, aiming to identify critical thresholds for distance protection and suggesting areas for further research.

## 1.3. Cyber Security

Power systems are undergoing fundamental changes in terms of digitalization, decarbonization, and decentralization. This phenomenon necessitated the extensive implementation of innovative digital technologies. Digitalization is facilitating the development of advanced and intelligent power grids,

while also giving rise to concerns regarding cyber security. Consequently, power grids are now more susceptible to cyber-attacks as a direct result of their growing reliance on digital technologies and equipment. Attacks on the power grid can potentially lead to devastating consequences for public safety, national security, and economic stability. Therefore, the cyber security of power grids has emerged as a critical issue that is being widely investigated in academic research.

The state-of-the-art research is currently examining the cyber vulnerabilities of new prominent technologies being integrated into power grids, assessing the impact of cyber-attacks on their operation, and creating defense strategies to protect them from attacks. The research includes state estimation and automatic generation control, optimal power flow, cyber security for Phasor Measurement Units (PMU), and power system communication protocols. Among them, research on the cyber security of High-Voltage Direct Current (HVDC) systems has become increasingly popular. While there has been extensive research on cyber security aspects of High-Voltage Alternating Current (HVAC), there is limited research that addresses the cyber security aspects of HVDC. Therefore, in this report, we investigate vulnerabilities and impacts of cyber-attacks on the performance of HVDC systems. This cyber security events protection of HVDC grids is presented in section four of the report and covers the following aspects:

#### **Survey of the state-of-the-art research on HVDC cyber security.**

This report provides a systematic literature review of the state-of-the-art research on HVDC cyber security. The scope of the survey includes cyber threats and vulnerabilities on HVDC grids, HVDC cyber-physical system testbed for cyber-attack experiments, and cyber-attack mitigation. Based on the systematic literature review, we provide a summary of the latest cyber security research on HVDC grids and recommendations for future research and implementation.

#### **Assessment of cyber-attack impacts on HVDC grids.**

We implement a Hardware in the Loop (HIL) experimental setup to assess the impact of cyber-attacks on the HVDC grids. Case studies of cyber-attacks were implemented using the Real Time Digital Simulator (RTDS) and HIL facility within the Electrical Sustainable Power Laboratory (ESP) lab at TU Delft. The analysis of the impacts of cyber-attacks is presented in this report, including physical anomalies and cyber anomalies. Subsequently, the experimental findings are utilized to formulate a potential strategy for mitigating and protecting an HVDC system from cyber-attacks.

#### **Anomaly detection for cyber-attack mitigation on HVDC grids.**

The state-of-the-art anomaly detections on HVDC grids under cyber-attack are mainly based on physical power system measurement, i.e., SCADA and PMU. The physical anomalies occurred after the cyber-attack had already impacted the physical HVDC grids, during the later stage of the cyber kill chain. The method was developed based on the characteristics of Operational Technology (OT) communication traffic, which originates from automated processes with deterministic and homogeneous behavior. The method identifies the anomalies based on traffic throughput using a Graph Convolutional Long Short-Term Memory. Subsequently, the results of anomaly detection are combined with the Traffic Dispersion Graph to identify the locations of anomalies. The method is utilized to detect anomalies by analyzing the recorded traffic using a Forensic Graph (FGraph) Model. The proposed FGraph model aligns with the objective of avoiding time delays in HVDC communication by utilizing historical OT traffic data. The results of the experiment indicate the proposed method has the potential to serve as an alternative solution for protecting HVDC systems against cyber-attacks, especially for the early stage of the cyber kill chain.

## 2. DC Fault-Ride Through Analysis

DC faults in HVDC systems can significantly affect AC stability, especially in the context of Multi-terminal DC (MTDC) systems, posing a threat to the operation and stability of the AC grid. Therefore, studying DC Fault Ride-through (FRT) is crucial for assessing AC system stability. Initially, a DC fault may appear as a sudden loss of power input or load disconnection, prompting primary control to restore power balance using available reserves (such as FCR and FFR) and inertia to maintain system stability. However, in many cases, HVDC system protection is designed to block converters when current peaks or power limits are exceeded, which may not effectively address power balance regulation on the AC side. Thus, coordinated action between AC and DC grids becomes necessary to sustain system operation and mitigate the impact of DC faults.

Normally, investigating such operations requires complex Electromagnetic Transient (EMT) models, as small-signal stability analysis may not adequately evaluate these events, and tools are constrained by model intricacies. Therefore, the initial studies in this chapter regarding DC protection impacts will be handled in EMTP software, where the converter models are built in a detailed manner. But, in the next stages of the project (WP6), RMS analysis will be carried out, where it will be possible to assess the system's behavior and gain an overview of the achievable DC protection results using RMS simulations. In other words, this will help determine how effective simpler analysis tools can be for this type of study.

The DC protection must be able to detect and clear faults to enable uninterrupted transmission of power within the grid, preventing disruptions to the stability of the AC system's transient, frequency, and voltage. In the North Sea Wind Power Hub (NSWPH) feasibility study, top priority has been given to maintaining frequency stability. The selected criteria revolve around permissible Temporary Stop (TS) and Permanent Stop (PS) of active power during a fault occurrence, along with the duration of active power TS [10]. These criteria directly impact the Frequency Containment Reserve (FCR) and Frequency Restoration Reserves (FRR) of interconnected onshore AC systems. From [5], Table 2-1 introduces the AC system criteria regarding the fault probability. The focus of the analysis performed in this chapter is regarding TP, where C&P actions are designed to retake the system operation according to grid requirements. The AC and DC busbars are configured to be single busbars, and the protection requirements are given as reference values introduced in Table 2-6.

**TABLE 2-1: AC SYSTEM CRITERIA ACCORDING TO THE FAULT PROBABILITY.**

FAULT PROBABILITY	CRITERIA
High (1 occurrence per year)	PS $\leq$ 1 GW and TS $\leq$ 1 GW during 150ms
Low (0.01-0.1 occurrence per year)	PS $\leq$ 2 GW and TS $\leq$ 2 GW during 150ms
Very low (0.0001-0.001 occurrence per year)	PS $\leq$ 3 GW and TS $\leq$ 3 GW during 150ms

The criteria for permanent stops (PS), which are linked to high-probability faults, have been carefully determined by considering the minimum Frequency Restoration Reserve (FRR) required by the connected countries, set at 1 GW. In situations involving low-probability faults, the maximum PS assumes that the connected countries will jointly utilize the FRR reserves up to 2 GW. In the rarest scenarios, where the probability of faults is very low, it is assumed that all countries will collectively maintain a Frequency Containment Reserve (FCR) of 3 GW, similar to the standards observed in the European area. Importantly, it's worth noting that the criteria for temporary stops (TS) and permanent stops (PS) regarding reactive power are closely linked with considerations of voltage stability [5].

In this report, we are focused on the analysis of temporary stops (TP), where the DC-FRT operation is able to restore the system operation after the contingency. The time of the ride-through is determined to be 400 ms, considering the fault inception, the isolation of the fault and the restoration to normal operation (considering the post-fault condition).

The strategy for DC Protection involves two main phases: fault clearing and fault recovery. Fault clearing focuses on interrupting fault currents and isolating failed or failing assets, while fault recovery deals with restoring power after faults are resolved. This may involve adjusting converter controls or reconfiguring switches. Various Fault Clearing Strategies (FCS) have been proposed, including Fully Selective (FS), Non-Selective (NS), and Partially Selective (PS) methods.

In the FS approach, protection is limited to specific sections like the line or busbar. On the other hand, NS protection covers the entire DC grid. Consequently, with NS-FCS or PS-FCS strategies, temporary power interruptions following a DC-side fault could exceed 3 GW, leading to around 3-4 frequency interruptions per year. Thus, these strategies may have the most significant impact on the AC grid.

The examination of DC faults encompasses a broad spectrum of stability analyses, affecting factors such as frequency, rotor angle stability, synchronization, and DC voltage control (specifically, converter-driven stability). Within this framework, this study focuses on developing detailed EMT models of Modular Multilevel Converter (MMC) converters utilizing energy-based control. These models are applied to MTDC grids configured in a bipolar manner.

Various control strategies, including grid-following (GFL) and grid-forming (GFM), as well as different protection schemes ranging from non-selective to fully selective approaches, are explored. Additionally, understanding the events that could trigger converter blocking and DC breaker tripping is crucial. DC breakers represent a significant advancement in DC grid technology due to their rapid actuation, operating within a time scale of a few milliseconds (3-10 ms). These components form the foundation of the EMT models necessary for studying specific grid events selected for analysis.

#### **Objectives of the DC FRT Analysis and Simulation Assumptions**

This subtask aims to evaluate the impact of the DC protection philosophies concerning Reliability and Resilience (R&R) for different grid characteristics, control strategies, converter configurations towards performance standards. First, the characterization of DC FRT is going to be carried out, considering the time scale of the protection sequence in different control strategies and then the analysis of different dynamics of the system are going to be included, such as frequency and rotor angle dynamics. From the AC side grid point of view, the grid characteristics include parameters such as inertia, Short Circuit Ratio (SCR), frequency dynamics considering synchronous generators and Power Electronic (PE) based grids. On the other hand, the DC side grid considers a MTDC minimum meshed system, focused non-selective protection philosophy since the impact of a DC fault is more evident in this kind of strategy. Also, different control strategies, as grid-forming (GFM) and following (GFL) are considered in the analysis, such that the behavior of the control coupled with the designed protection strategy can be understood, and possible interactions can be mitigated. The operational limits of the converters are also investigated in a DC FRT operation, so the triggering of specific strategies for operational security are activated, such as current limitation, and how the trigger of such strategies affects the stability of the system and what are the boundaries in this level of operation.

The subtask is focused on the characterization and proposition of DC fault ride-through for AC/DC systems according to suitable solutions for RMS analysis and EMT simulations to be detailed in WP6 and WP7. The proposed assessment can be done considering different system configurations:

1. Standard configuration (system strength and traditional C&P coordination)
2. Different control strategies for the converters connected to the AC grid (GFL and GFM)
3. Different AC grid configuration, AC infinite bus and synchronous machines
4. Oversize the converters
5. Power reserves on the AC grid (storage, FFR)

Within the same framework, the introduction of novel concepts that account for emerging technologies, such as AC storage given by battery storage system or even a pumped storage interfaced by power converters (fast action response), and the subsequent comparison of these concepts in terms of performance versus cost are anticipated. Consequently, the culmination of this subtask yields methodologies for the efficient coordination of AC/DC controls and DC grid protection schemes.

The general configuration scenario of studied simulation in this chapter is introduced next:

**An exemplary case under scrutiny is the MTDC with a bipolar configuration, the investigation addresses the scenario where a DC fault occurs on one pole, exploring how the unaffected pole mitigates the fault impact on the AC grid.**

The exploration also delves into the necessity of incorporating diverse control strategies in the converter station to enhance DC FRT performance on the DC side. This analytical perspective proves to be a noteworthy consideration in the broader context of AC stability analysis for DC FRT.

When referring to DC protection strategies for MTDCs, the non-selective protection philosophy is considered the most critical one, since if a fault happens the whole DC grid is affected. Non-selective strategies are considered as 1 protection zone, which will result with more impacts when compared to other protection strategies. Therefore, the non-selective protection strategy has been selected to be the main focus of DC FRT analysis in this chapter. The comparison with other protection strategies as fully selective strategy is not really relevant to characterize the profile of power and voltage curves for simulations aimed at RMS analysis, since the converters in that scenario may not be blocked and the time of loss infeed can be drastically reduced, minimizing impacts on AC grid system stability. In this context, the examinations conducted on FS protection strategies revealed negligible impacts on the AC grid side, as transients were confined within the operational time of the DCCB. Additionally, the utilization of reactors in such applications significantly constrains short-circuit current peaks, rendering the FS protection strategy a less appealing option for furnishing guidelines of system impact in subsequent working packages of the project. It's important to note that FS protection involves greater design complexity, factoring in costs and additional equipment like reactor design, protection sensitivity, and short-circuit current values. These aspects can be evaluated later through the use cases in the next working packages.

For practical considerations, the chosen DC network type will be exclusively the minimum meshed Multi-Terminal DC (MTDC) grid, as outlined subsequently as it is considered a more complex configuration from the point of view of power flow. Furthermore, in this configuration it is possible to continue with the power supply after a fault even if it is reduced, when compared to the linear and radial configuration, which simply cut off the power flow in the system, thus it is possible to investigate the temporary stop of power more adequately.

This selection stems from the intricate nature of this configuration, elucidated in the analysis conducted in Task 2 of this project. In that phase, a 4x4 matrix was established to scrutinize various High Voltage Direct Current (HVDC) system configurations and topologies. The MTDC stations are implemented in a bipolar configuration to accommodate diverse scenarios of DC faults, where power flow is not entirely disrupted. This arrangement enables the concurrent examination of the unaffected

pole and its impact on the AC grid. Depending on the control strategy employed in the converters, the unaffected pole can either provide support to the system during contingencies or exacerbate its operational challenges during such events. Consequently, the analysis of the bipolar configuration is deemed of paramount interest.

The adoption of a bipolar configuration is expected to be prevalent due to its inherent redundancy advantages, notably single pole fault tolerance. Noteworthy instances include the Viking Link, a recently commissioned converter station in a bipolar configuration connecting the UK and Denmark [11]. Additionally, the EuroAsia Interconnector, scheduled for commissioning in the upcoming years, is designed with the same configuration, aligning with other listed bipolar projects [12].

Regarding the fault types, they can be described as line fault, active fault on DC breaker, busbar fault, DC breaker failure, spurious trip, sympathetic trip, and converter failure. The most common are converter failures (3 occurrences per year) and line faults (0.035 failures per year). Therefore, the investigation will be on cable DC faults, pole to ground faults since a pole-to-pole fault would result in permanent stop of power supply. The analysis is performed in bipolar configuration pole to ground fault, where the behavior of the healthy pole can be detailed in different control configurations.

### Configuration of the Case Scenarios

This subtask considers different AC grid configurations connected to a DC meshed grid. The main objective is to perform the stability and operational analysis of the AC grid when a DC fault occurs, highlighting how each AC grid is impacted by this perturbation. Therefore, 4 different AC grid configurations are selected to compose the case scenarios of this study, they are defined in Table 2-2.

**TABLE 2-2: THE SELECTED CASE SCENARIOS.**

CASE	AC GRID	CONTROL STRATEGY	COMMENTS
01	AC grid (infinite bus) – strong grid	Bipolars in GFL	No frequency dynamics considered (state of art)
02	AC grid (infinite bus) – weak grid	Bipolars in GFL and GFM	-Minimum voltage impact (no stability issues) -Electro-mechanic dynamics in evidence (frequency stability)
03	Synchronous generator	Bipolars in GFL and GFM	Study of electrical area: -Frequency stability analysis (ROCOF and nadir); -Rotor angle stability issues
04	Power Electronic based grid	Bipolars in GFM	-Frequency and rotor angle stability analysis -Fault currents levels, blocking problems and stability issues

The case scenarios are formulated based on the configuration of the AC grid, where the system's behavior in response to a contingency is defined by its characteristics and devices. The first scenario entails the examination of a strong grid (high SCR level ( $SCR > 3$ )), modeled as an infinite bus. In this scenario, the system effectively responds to power perturbations, ensuring voltage and frequency stability. The analysis explores power and current peaks during a fault, assessing the impact on DC protection to inhibit faulty lines and block MMCs. Concurrently, the AC grid experiences perturbations due to an instantaneous change in power demand, involving load increases in the initial transient and load reductions after the DCCB is opened. This is considered a standard case to define the behavior DC FRT in HVDC systems, since it has been widely studied in literature resulting to be the state of art in this context. Nevertheless, this scenario is going to be used to perform the characterization of the

DC FRT for HVDC systems controlled in GFL connected to strong grids, where no stability issues are expected.

The second scenario considers a weak grid (low SCR level ( $SCR < 3$ )), also modeled as an infinite bus but with increased impedance between the converter and the grid. This configuration challenges the grid's ability to transfer power, necessitating more effective reactive power for voltage control. The reduced speed dynamics in this scenario prompt an investigation into power response implications, with a comparative analysis incorporating the implementation of GFM control. The idea is to characterize the GFM control sequence in DC FRT, therefore the speed dynamics of grid forming converters are taken into account to adapt the contingency sequence, such that each relevant phenomena that appears in this condition is assured to be analyzed. Then, strategies and recommendations are proposed to ensure suitable DC FRT operation.

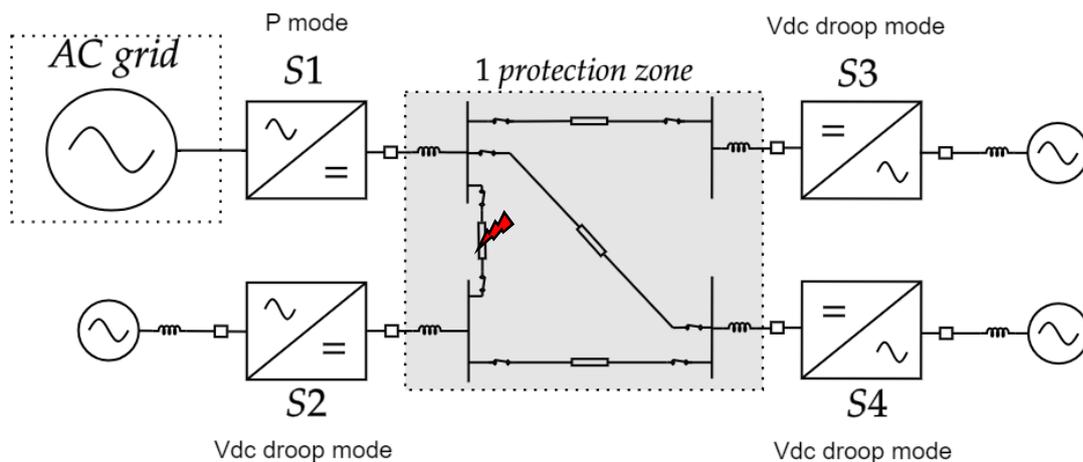
The third scenario introduces frequency dynamics by the connection of a rotating machine in the AC grid, allowing for an assessment of the impacts on the Rate of Change of Frequency (RoCoF) and frequency nadir, meaning frequency stability analysis. Therefore, the interactions of the GFM converter connected to the AC grid can be better understood in the DC FRT context. The electrical distance of the synchronous machine to the converter is evaluated to determine the RoCoF impact in different impedance values. Additionally, rotor angle stability within predetermined angle limits during a fault can be analyzed considering GFL and GFM control strategies.

The fourth scenario comprises a fully power electronic grid, enabling the assessment of low inertia features and control interactions between converters. The frequency stability assessment is also considered here as done in the third case scenario. In this case, the limited capacity of the converters to operate overload can be highlighted when the fault occurs, by resulting in limited overcurrent which can jeopardize the blocking of the faulty converters. The analysis considers the rapid action of protection schemes in collaboration with control strategies, thereby facilitating the formulation of recommendations for control and protection actions.

The detailed analysis of each case scenario is carried out in the following sections of the DC protection philosophies chapter.

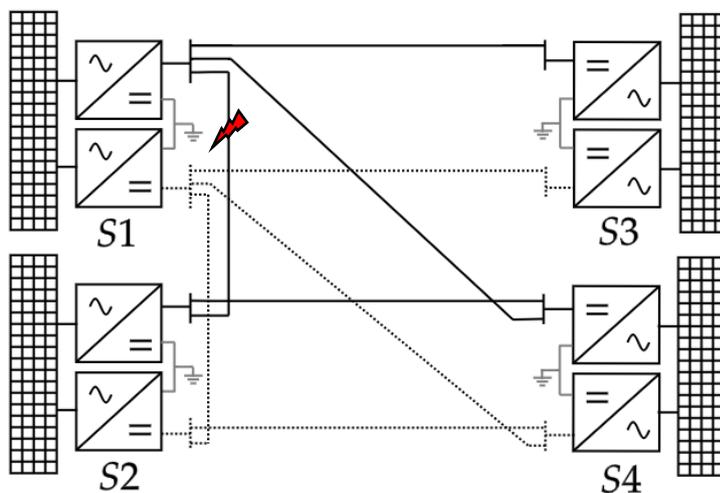
#### Reference Simulation Definition

In this section, the reference grid scenario is detailed, such that all case scenario simulated in this chapter follow the parameters introduced here. The basic scenario is composed of an AC grid connected into the meshed MTDC grid as depicted in Figure 2-1. The AC grid is configured according to the different case scenarios, and the MTDC grid is composed of 4 stations: S1, S2, S3 and S4 and they are connected such that, a minimum meshed configuration is obtained. The cables that compose the MTDC grid are modelled as frequency dependent single core cables with a metallic sheath to have a more homogeneous charges distribution with a length of 140 km. Further cable modelling details are not considered since these are out of the scope of these studies. The S1 station is in power control mode (P-mode), being the focus of the study and it can change its control structure according to the scenario analysis; Stations S2, S3 and S4 remains in DC voltage control mode (Vdc-mode), they are controlled by a droop strategy, where the droop gain is  $k_p = 10$ , and they are connected to their respective AC voltage sources, representing connection with different AC areas.



**FIGURE 2-1: GENERIC ELECTRICAL MODEL OF THE STUDIED SYSTEM: AC GRID CONNECTED INTO THE MESHED MTDC GRID.**

The MTDC grid is a minimum meshed one in a bipolar configuration, referring to the classification developed in Task 3.1 on the AC/DC system architecture matrix, which is the AC1 (all separated grids) configuration related to the AC side of the grid and the DC4 (meshed grid) configuration related to the DC side of the grid. The electrical model of the bipolar configuration is introduced in Figure 2-2, where the positive pole is presented with continuous line, the negative pole is presented in dashed line and the return is grounded presented in grey line. The DC fault is performed at the middle of the positive pole cable that interconnects the station S1 and station S2.



**FIGURE 2-2: THE BIPOLAR CONFIGURATION OF THE MTDC MESHED GRID.**

The non-selective protection configuration is implemented by means of a DC break in the DC output of each converter with a line inductor of 200 mH, composing 1 zone protection as shown in Figure 2-1. Therefore, in a DC fault, the faulty pole restricts the operation of all stations in the MTDC until the fault is isolated. The DC fault can be isolated by using switches that can be operated once the current on the cable is extinguished. The switches are included in each extremity of the cables in the MTDC grid, therefore, after the DCCB operation, the faulted cable is isolated, and system operation is restored. The protection relays are able to detect the fault and send the tripping signal to open the DC breakers in 10 ms [13, 14]. This set up allows the analysis of a temporary loss of power infeed due to a fault in the cables or lines interconnecting the DC grid; consequently, the DC fault ride through (FRT) can be characterized to be further analyzed in order to identify possible improvements in terms

of reliability and resilience. The DC power flow is defined in Table 2-3, where negative values designate power injected into the DC grid.

**TABLE 2-3: INITIAL POWER FLOW IN THE MTDC.**

STATION (BIPOLAR)	P	Q
Station 1	-1200 MW	400 MVar
Station 2	1200 MW	400 MVar
Station 3	800 MW	400 MVar
Station 4	-800 MW	400 MVar

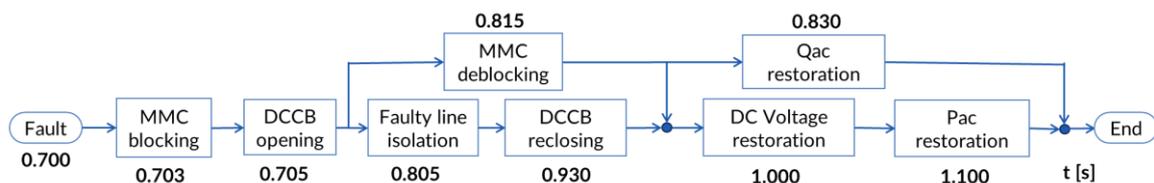
The AC power flow will depend on the devices considered in each case scenario, but the power flow in Station 1 is defined according to Table 2-3, per station, where negative values indicate power flowing to DC grid.

**TABLE 2-4: INITIAL POWER FLOW IN AC GRID.**

STATION	P	Q
Positive Pole – Station 1	-600 MW	200 MVar
Negative Pole – Station 1	-600 MW	200 MVar

The triggering of the DC breakers is done automatically by the fault detection strategy, but a communication among the stations in the MTDC is required, so that it is possible to coordinate the restoration process of the DC breakers, considering the information on the DC voltage and DC current levels and fault status on the DC side. Communication among the converters in the MTDC is assumed with no time delay. This is a simplification to model the fault restoration process, where it is possible to deblock the MMC, to reactivate active and reactive power control, to restore DC voltage control and to reclose the DCCB performing the full restoration process in 400 ms, as established in temporary faults.

The reference scenario establishes a DC fault in the positive pole to the ground (1 mΩ resistance) in the cable between stations 1 and 2 at 0.7 s of simulation. It is considered that system is in steady state operation at the moment of the fault, and for simulation purposes, it is considered that the faulty cable is isolated 105 ms after the DC fault (the faulty cable is disconnected from the stations terminals, resulting in a radial system), so the DCCBs can be reclosed and the power in the non-faulty cables are reestablished. Accordingly, the FRT is divided into two parts, the fault clearing and the fault restoration, and they have been detailed in the next subsections. The reference scenario considers a temporary loss of infeed, where the power is fully recovered in 400ms, to perform the protection coordination sequence that is introduced in Figure 2-3. This is simulating the behavior of a temporary stop, where the DCCB are placed on the converters terminals (non-selective protection philosophy).



**FIGURE 2-3: PROTECTION COORDINATION SEQUENCE.**

According to Figure 2-3, from the DC fault to active power restoration 400ms is the required time to perform the whole protection sequence coordination. It is considered that the DCCB is able to open the short circuit in 10ms. Once the DCCB is opened, it is possible to perform parallel actions: deblock the converters (positive pole) and to initiate the isolation of the faulty line, which is done by switches that isolates the faulty line resulting in a linear configuration for the DC grid. After the MMC is deblocked, the converter can restore reactive power and starts the operation as a STATCOM. In parallel, when the DCCBs are reclosed, the DC voltage and the active power can be restored respectively, bringing the system back to the pre-fault operating point.

The critical points in this sequence are described as:

- The ability to isolate the fault (DCCBs isolate the DC side in 10 ms and then the faulty cables are isolated by switches, reconfiguring the system), which relies on the identification of the fault location.
- The ability to send the command to open the lines; the ability to detect the opening of the DCCB.
- And the ability to send the command to deblock the MMC.

Therefore, considering a fast isolation capability and deblocking action, it is possible to perform the complete restoration sequence in 400ms.

Stations S1, S2, S3 and S4 are in bipolar configuration, resulting in 2000MVA of nominal power at each station. The values presented in Table 2-5 are used as the base values for per unit transformation for each converter.

**TABLE 2-5: MMC PARAMETERS IN ALL STATIONS.**

PARAMETER	VALUE
$S_{nom}$	1000 MVA
$V_{ac}$	400 kV
$V_{dc}$	525 kV
Transformer	0.001+0.18j pu
Arm inductance	0.15j pu
Conduction losses per SM	0.001 $\Omega$
Number of SM per arm	200

Therefore, the per unit values of the simulations are calculated based on the following base:  $S_{base} = 1000 \text{ MVA}$ ,  $V_{ac,base} = 400 \text{ kV}$ ,  $V_{dc,base} = 525 \text{ kV}$  and  $f_{base} = 50 \text{ Hz}$ . The HVDC stations are equipped with MMC blocking protection, assuring safe operation according to current and voltage limits, the blocking parameters of the MMC's are introduced in Table 2-6. These protection parameters are established in Table 2-6 being considered the pass/fail criteria for the related variables, they are maintained for all simulations in this chapter.

**TABLE 2-6: MMC BLOCKING PARAMETERS.**

PARAMETER	VALUE
Power limitation	$I_{ac,max} = 1.2 \text{ pu}$ , with $I_d = 1.2 \text{ pu}$
DC current protection	$I_{dc} = 2 \text{ pu}$ (blocking time 40 $\mu\text{s}$ )
IGBT current protection	$I_{arm} = 4000 \text{ A}$ (blocking time 270 $\mu\text{s}$ )
DC voltage protection	$0.8 \leq V_{dc} \leq 1.2 \text{ pu}$ (blocking time 500 $\mu\text{s}$ )
AC voltage SAG protection	$V_{ac} < 0.8 \text{ pu}$ , (blocking time 40 ms)

Regarding the grid requirements, in normal operation the

Regarding the grid requirements considered in the simulations, the normal operation of the system considers maximum of 10% variation for DC voltage [15]. The region of continuous operation in AC voltage is given as  $0.95 pu \leq V_{ac} \leq 1.05 pu$ , variations between  $5\% \geq \Delta V_{ac} \geq 10\%$  cannot persist more than 10 minutes. The adopted frequency standard is  $57.5Hz \leq f_g \leq 52 Hz$  for continuous operation considering weak grids [16].

The MMC model follows the one developed in [17, 18, 19], where the details of the control structure can be found. The MMC is controlled using the Energy based control as introduced in [20, 21]. When the converter is in GFL control, the external control loops are given by PI controllers to control the active and reactive power (P-mode), or the DC voltage and reactive power (Vdc-mode). The external loop provides the references for the inner loop, the current control loop given by a PI controller, where the output are the modulation indexes. Figure 2-4 introduces the global control structure of the MMC, where more details can be found in [18]. The time constant of the current control loop is on the order of  $10^{-3} s$ , while the outer loops as the AC power and DC power controllers are about  $10^{-2} s$ . The time constant of the DC voltage controller and the energy controller are on the order of  $10^{-1} s$ .

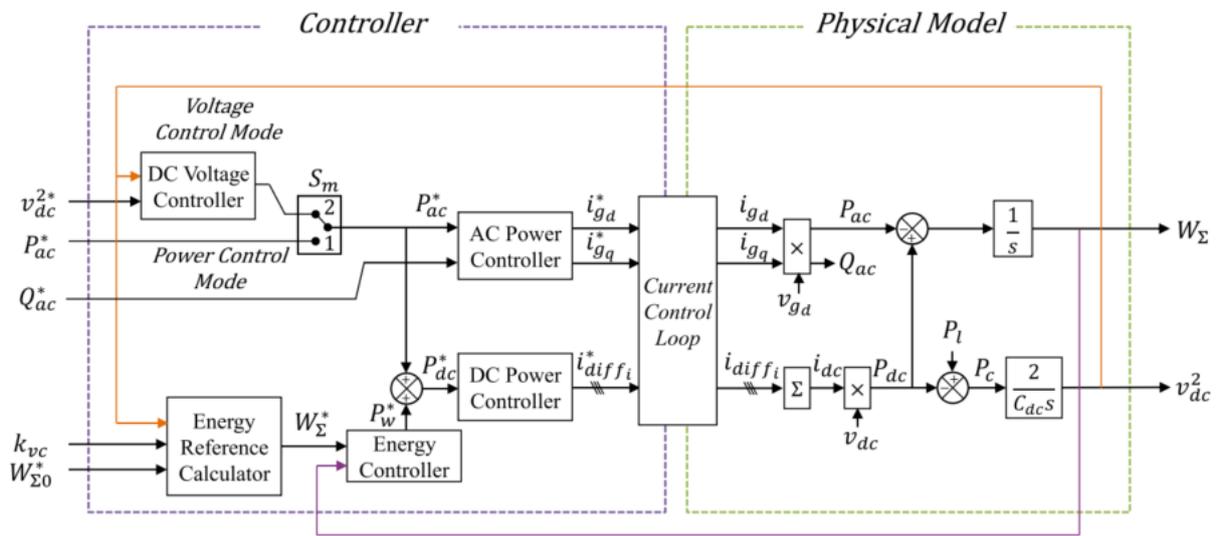


FIGURE 2-4: GENERAL CONTROL STRUCTURE OF THE MMC IN GFL.

### Definition of GFM

The grid-forming control (GFM) in this chapter is implemented as a Virtual Synchronous Machine (VSM) with the PLL tracking the grid reference as developed in [22] and presented in equation (1). The GFM control has undergone comprehensive scrutiny within the framework of Task 3.2 and is presently implemented as a designated control paradigm for AC/DC system architectures. This integration is imperative for the systematic evaluation of the intricate interactions between control strategies and protection schemes. Foreseen as a pivotal solution, the GFM control is poised to experience increased applicability in the foreseeable future. The inner voltage and current control are implemented according to [23], using inverse current control loop, which allows the application of the Current Saturation Algorithm (CSA), used for current limitation purposes. Better details can be found in the control functionalities of Task 3.2.

The swing equation as described next according to [24]:

$$\dot{\omega}_{vsm} = \frac{1}{2H} [P^* - P - D_p(\omega_{vsm} - \omega_g)] \quad (2.1)$$

where  $P$  is the measured power in the converter,  $P^*$  is the power reference,  $\omega_{vsm}$  is the computed frequency by the VSM, and  $\omega_g$  is the grid frequency computed by the PLL.  $H$  is the inertia constant and  $D_p$  is the damping factor. The phase angle is computed as the integral of the produced virtual frequency  $\delta_{vsm} = 2\pi f^* \int \omega_{vsm} dt$ .

The voltage control of the GFM is given by a droop relation with the reactive power and it is described as:

$$V_d = V_d^* + m_v(Q_m - Q^*) \tag{2.2}$$

where  $V_d^*$  is the AC voltage magnitude reference,  $m_v$  is the voltage droop coefficient,  $Q_m^*$  is the reactive power reference and  $Q_m$  is the measured power.

When the converter is in GFM control, the AC inner loop is given by the voltage control, without the original current control loop. The Active power control is given by the swing equation written in equation (1), which provides the power angle of the converter, and the Reactive power controller is given by the voltage droop expressed in (2), which provides the voltage magnitude. Therefore, now, the converter has a voltage source behavior. The external loops are the same and they are given by the DC voltage controller and the energy controller. The general control structure of the MMC in GFM control is depicted in Figure 2-5, as developed in [25, 26].

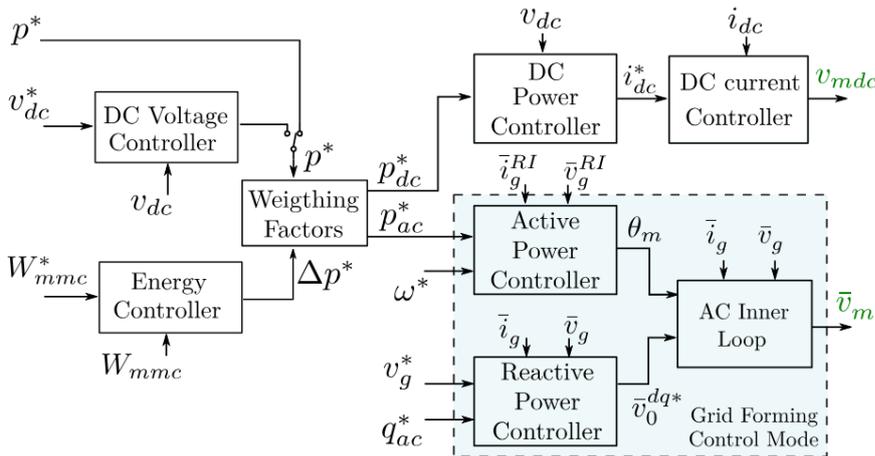


FIGURE 2-5: GENERAL CONTROL STRUCTURE OF THE MMC IN GFM.

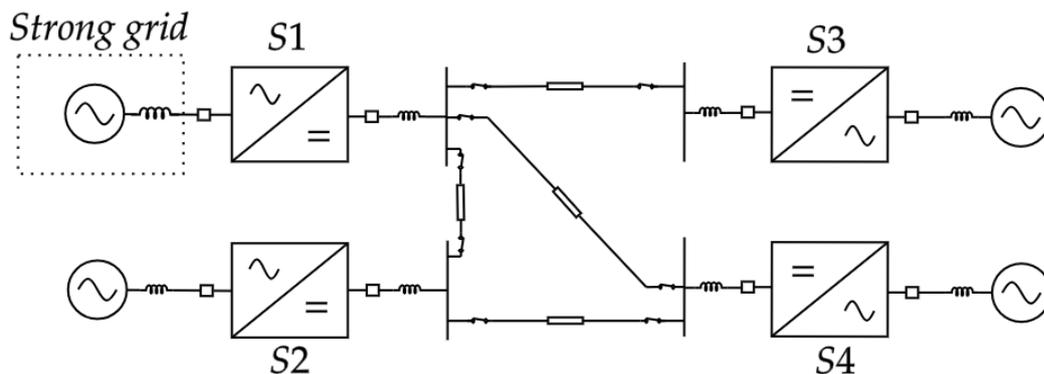
In this case an inverse current control loop and a virtual impedance strategy are implemented to control the limits of the converter’s current (current limitation control), which is developed in [23]. This is necessary to understand the dynamic behavior of the converter in case of grid events (like contingencies and Low Voltage Ride-Through (LVRT) operation), where peaks of current may occur, and the converter may limit its current contribution to events. Specifically, the LVRT operation of grid-forming converters will provide a high contribution of reactive power to provide support to the grid, which can also activate the current limitation control.

## 2.1. Strong Grid Scenario

The first scenario involves a strong grid, conceptualized as an infinite bus with a series impedance, thereby defining a Short Circuit Ratio (SCR) for the system, in this case SCR = 3. The AC grid is connected to Station 1, where converters in a bipolar configuration are implemented with the GFL control strategy, as illustrated in Figure 2-6. This scenario represents the simplest form of system architecture,

utilizing an equivalent grid. Consequently, an in-depth analysis of this case enables a lucid understanding of the converter station's responses and interactions with the AC grid.

The primary focus of this investigation lies in scrutinizing the power profiles during a fault, the subsequent recovery process, and the system restoration process. The evaluation encompasses an assessment of current levels to delineate operational limits and ascertain the blocking time of the converters. Additionally, key DC variables such as DC voltage and DC currents are depicted, shedding light on the FRT capability of this architecture in the context of DC faults. Here, a DC pole to ground fault is simulated as described in the reference case scenario. The coordination sequence for this case was introduced in Figure 2-3.



**FIGURE 2-6: ELECTRICAL MODEL OF STRONG GRID CONNECTED TO THE MESHED MTDC GRID.**

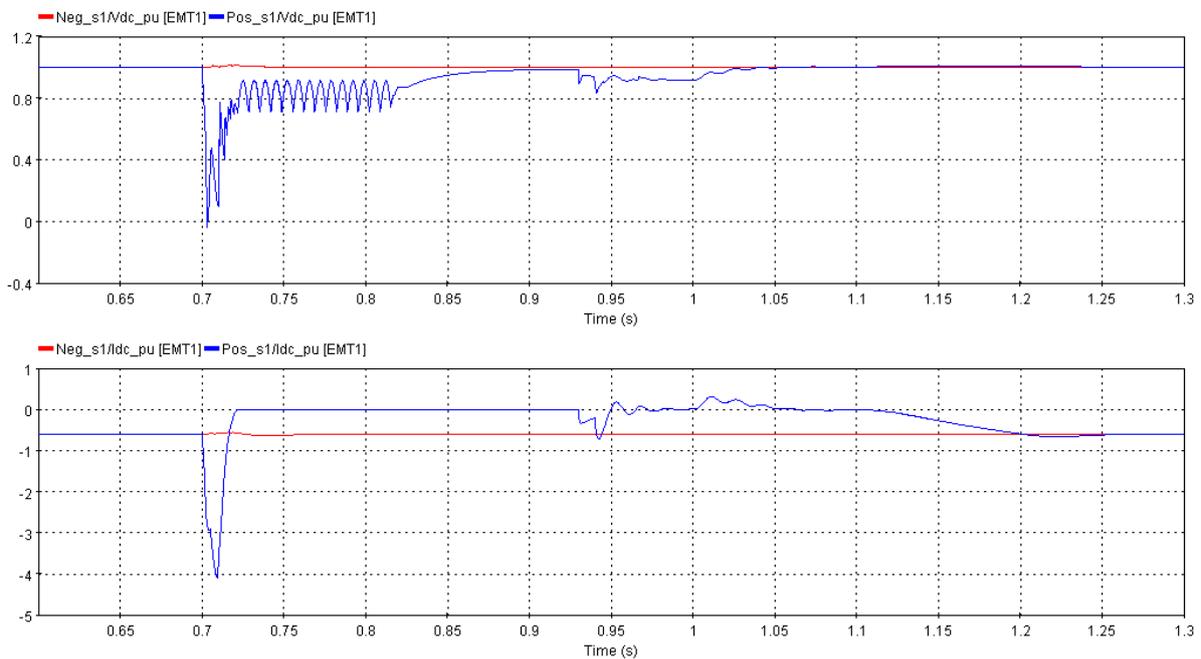
The simulated contingency sequence starts with the DC fault at the middle of the cable of the positive pole interconnecting station 1 and station 2 of the minimum mesh DC grid. The first protection action is the blocking of the converter: it is the bypass of the IGBTs in the converter submodules, by means of thyristors that will turn the MMC behavior to that of a diode rectifying unit once a current threshold is reached by the fault current flowing through the converter. Converter blocking is a consequence of the fault current that surpasses a threshold based on the IGBT overcurrent capabilities. The location of the fault has an important influence on the resulting operation of the DC FRT operation, given by the reaction of the DC breakers and the blocking of converters, also related to the level of the DCR installed in the DC meshed grid. Therefore, to determine the worst-case scenario for fault location is out of the scope of this report, but the following paper can provide a good insight on how fault location can impact the system in general [27].

After 10 ms, the DCCB will receive the tripping signal from protection relays and open the DC circuit. By opening the DC circuit, the fault current will be extinguished once the DC circuit is discharged. Only when the fault current reaches a level below 1 pu, the deblocking of the converter would be possible. In this case, it is done 105 ms after the breaker opening, when the fault current is zero. Once the MMC is deblocked, it is able to follow control actions; nonetheless, it would only exchange energy with the AC side. Thus, STATCOM operation can be started at this point. In this case, this operating mode is activated at 15 milliseconds after the deblocking, giving support to the AC voltage at the PCC. The only active power flow at this stage is the one that compensates for the switching losses and keeps the converter capacitors at good operating levels due to the energy control.

The next control action is reconnection to the DC system by reclosing the DCCB, that enables the restoration of DC voltage. The DC voltage restoration is provided by the stations S2, S3 and S4 that operate in V<sub>dc</sub>-mode, and therefore the impact on the faulty pole due to this control action is minimum on station S1. In the proposed protection sequence this occurs 100 ms after the DC voltage is restored.

Figure 2-7 introduces the DC voltage profile and the DC currents in the healthy pole Neg\_S1 (in red) and in the faulty pole Pos\_S1 (in blue). The coordination sequence can be clearly depicted by the behavior of the DC voltage, where a huge drop to zero happens at the moment of the DC fault. The MMC is blocked after approximately 2.5ms of the DC fault by overcurrent protection, where the protection parameters are presented in Table 2-6. The DCCB is opened after 10 ms and then the converter operates in diode rectifier mode. At 0.815s of simulation, the MMC is deblocked since the fault has been cleared, and 15ms later the reactive power is restored, so the converter can provide voltage support to the AC grid. At 0.930s of simulation the DCCB is reclosed and after 70ms the DC voltage is restored, so the stations S2, S3 and S4 share power to control DC voltage in its reference. Finally at 1.1s of simulation the active power is restored for all stations, bringing the system to the original operating point. The DC current of the faulty pole reaches 3.24pu at the moment of the fault, but it is interrupted when the DCCB opens.

Once the MMC is deblocked, the DC voltage cannot be controlled by the DC voltage control in the meshed DC grid, then its dynamics will be governed by the energy in the converter submodules capacitors. During this period, the internal energy control is also not working since the DC side is disconnected (internal energy dynamics will be detailed later), but no impacts in DC voltage stability is seen when the converter is in GFL control (stability issues will appear when the converter is in GFM control). The AC voltage level that is increased considering the reactive power support from STATCOM operation, but also because of the reduction of active power supply. Next, when the DCCB is reclosed, the DC voltage control in the positive pole converter is reestablished, where a transient event that reshapes the DC voltage profile into the controlled value.

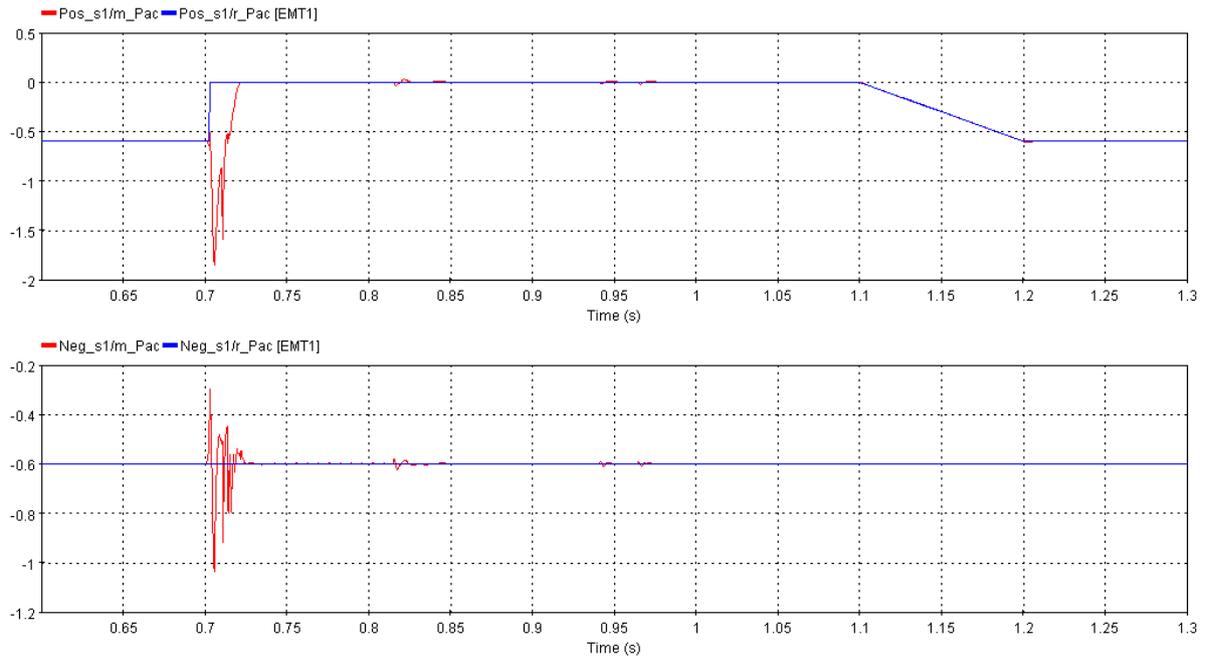


**FIGURE 2-7: DC VOLTAGE AND DC CURRENT OF STATION 1 IN PU, NEGATIVE POLE IN RED AND POSITIVE POLE IN BLUE.**

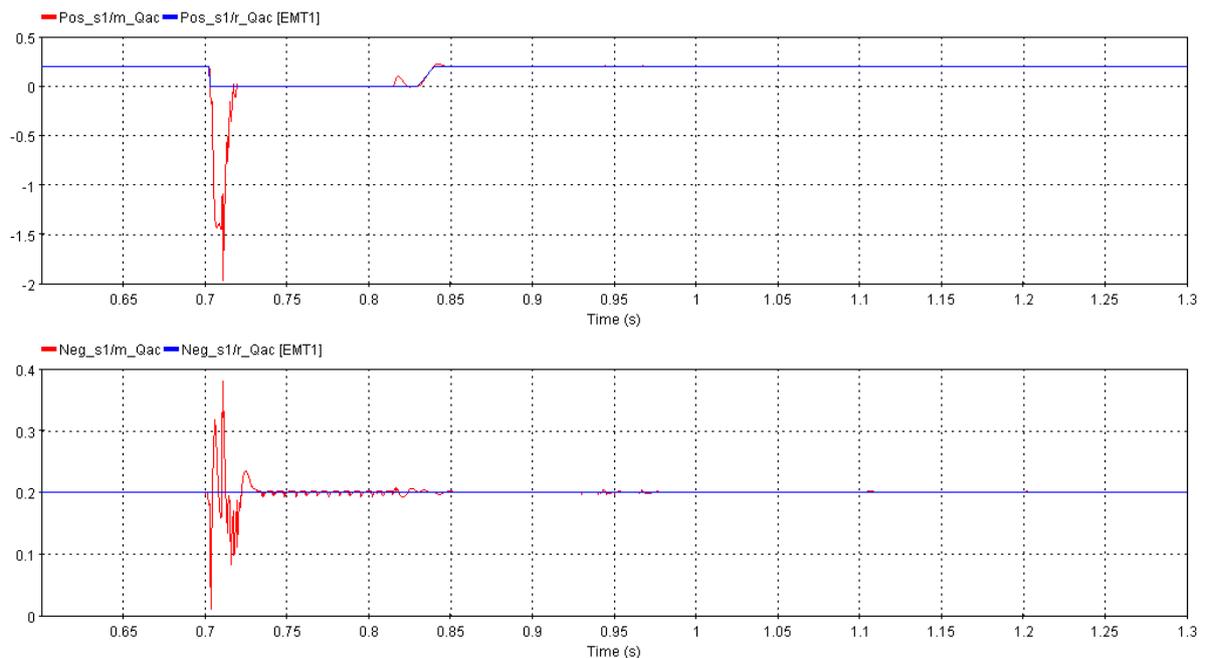
The active power profile of the converters Pos\_S1 and Neg\_S1 from station 1 are depicted in Figure 2-8. The healthy pole Neg\_S1 experiences a fast power transient during the fault, with an initial overshoot close to +0.3 pu of variation regarding the reference and then -0.4 pu above the reference, before the DCCB opens and power flow returns to the steady state operation. The faulty pole has a huge power transient of 2 pu, then going to zero power when the DCCB opens. When the converters

are deblocked, a fast but small transient appears, not impacting the system in any means, which indicates a smooth transition to restoration process. The faulty pole active power is restored in 1.1s of simulation, following the ramp restoration reference.

The reactive power profile of station S1, given by the Pos\_S1 and Neg\_S1 poles are depicted in Figure 2-9. Concerning reactive power, the peak of the faulty pole reaches -2 pu and it goes to zero when the DCCB is opened, while the healthy pole has oscillations around 0.2 at the moment of the fault that is reduced when the converter is in diode rectifying mode. The fault pole presents a small transient once the MMC is deblocked, followed by the reactive power restoration, where the reactive power is again controlled in the desired reference.

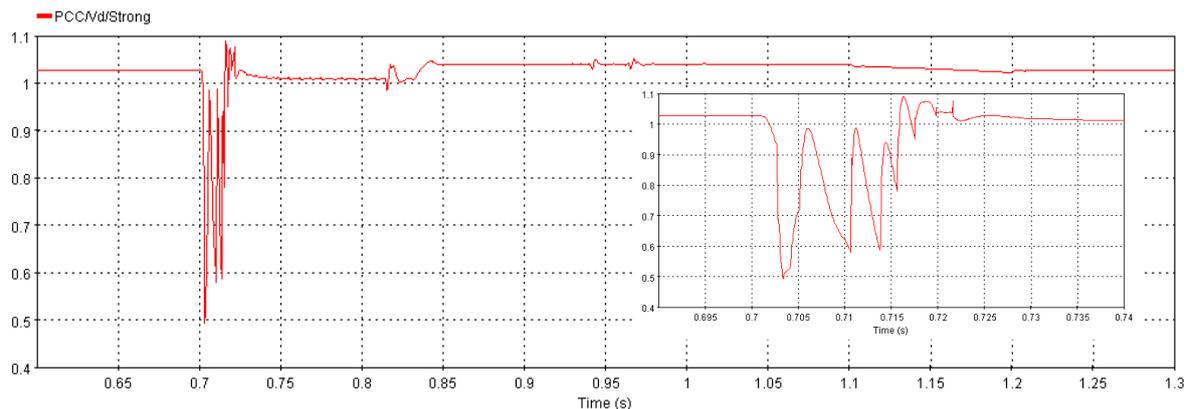


**FIGURE 2-8: ACTIVE POWER PROFILE IN POS\_S1 AND NEG\_S1, AND THEIR REFERENCES.**



**FIGURE 2-9: REACTIVE POWER PROFILE IN POS\_S1 AND NEG\_S1, AND THEIR REFERENCES.**

Figure 2-10 presents the AC voltage profile during the DC FRT. It can be noticed that the AC voltage is slightly disturbed at the moment of the fault, and it causes the AC grid voltage to sag to no less than 0.5 pu for 10ms, which results in impacts on the power quality indexes of AC grid and also can drive to triggering LVRT operation. It can be concluded that DC fault can affect the voltage in the AC grid according to the level of the voltage sag, nevertheless voltage disturbance occurs in order of tens of milliseconds, which can be considered too fast to impact the voltage stability in general. This is the expected result from the literature point of view, where the impacts on the system stability appear and the behavior of power profiles and DC voltages are given as presented in the state of art of HVDC systems.



**FIGURE 2-10: AC VOLTAGE ON THE PCC.**

The characterization of the power profile and DC voltage of the stations can help considerably in the construction of simulations for RMS analysis. The power profiles can be used as input for the RMS simulation, disregarding fast transients, such as the power peak during DC fault. In this case, the power curves obtained at this stage of the project can be used in WP6 to obtain the RMS model of the system. Nevertheless, it becomes clear that the fully selective protection philosophy has no impact on the composition of the power curves for RMS analysis, as it is possible to restore the power within a few milliseconds, which really has no impact on RMS simulations.

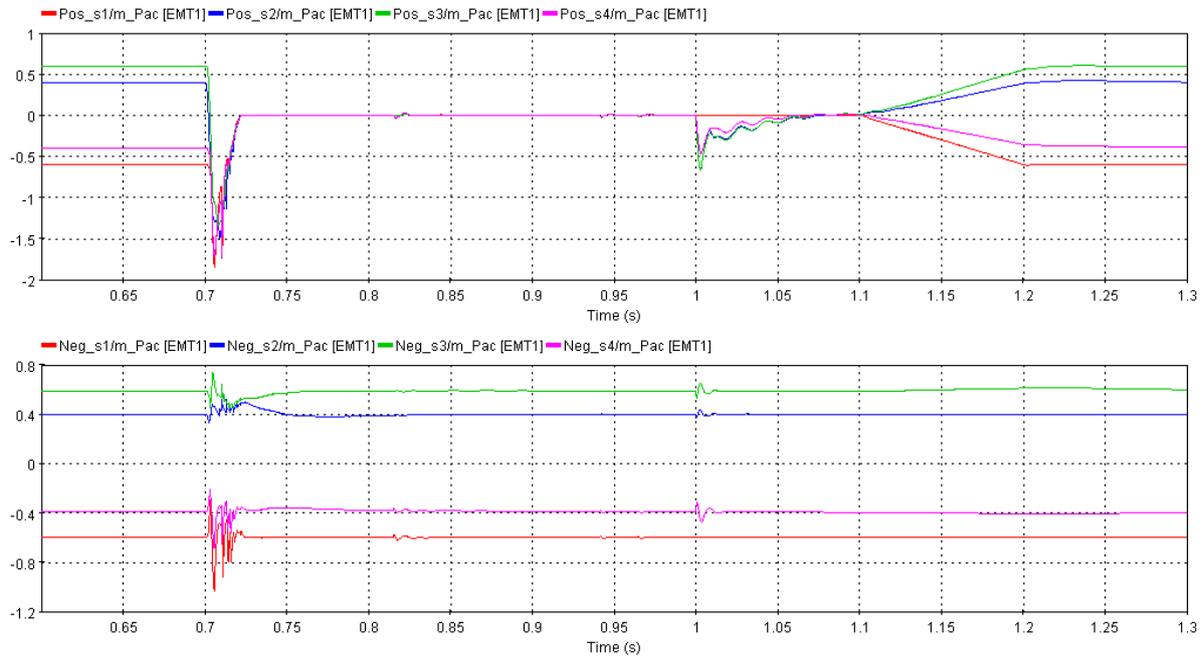
The DC FRT of the AC/DC system can be identified by the power profile of the faulted and healthy poles as depicted in Figure 2-11. The trapezoidal profile can be distinguished from the positive pole profiles. Furthermore, each of the described protection sequences can be identified. In the positive poles, the first peak is caused by the fault current, which then reduces following the voltage drop at the PCC. When the DCCB opens, a second transient occurs due to the interruption of the fault current and recovery of the AC voltage. The healthy pole will have an impact as well, since the perturbations of the AC grid voltage are propagated to the healthy pole, although they are naturally smaller. After this sequence of actions, a steady state is reached.

The faulty poles power is very high during the fault but falls to zero once the DCCB opens. Stations S1, S3 and S4 experience a considerable transient at 1s of simulation when the DC voltage is restored, so they share power to control the DC voltage. Then, at 1.1s the active power of the converters was recovered to steady state again. The healthy converters experience only a small transient peak during the fault, but they are not affected during the DC FRT restoration process. In this case, it is clearly seen the trapezoidal shape of the power for the DC FRT operation where the full power is restored.

The restoration process starts with the MMC deblocking. The reactive power restoration and the DCCB reclosing produce small transients that are transmitted from the faulted pole to the healthy poles via AC grid voltage. The next considerable power transient can be identified at 1 s of the simulation, which

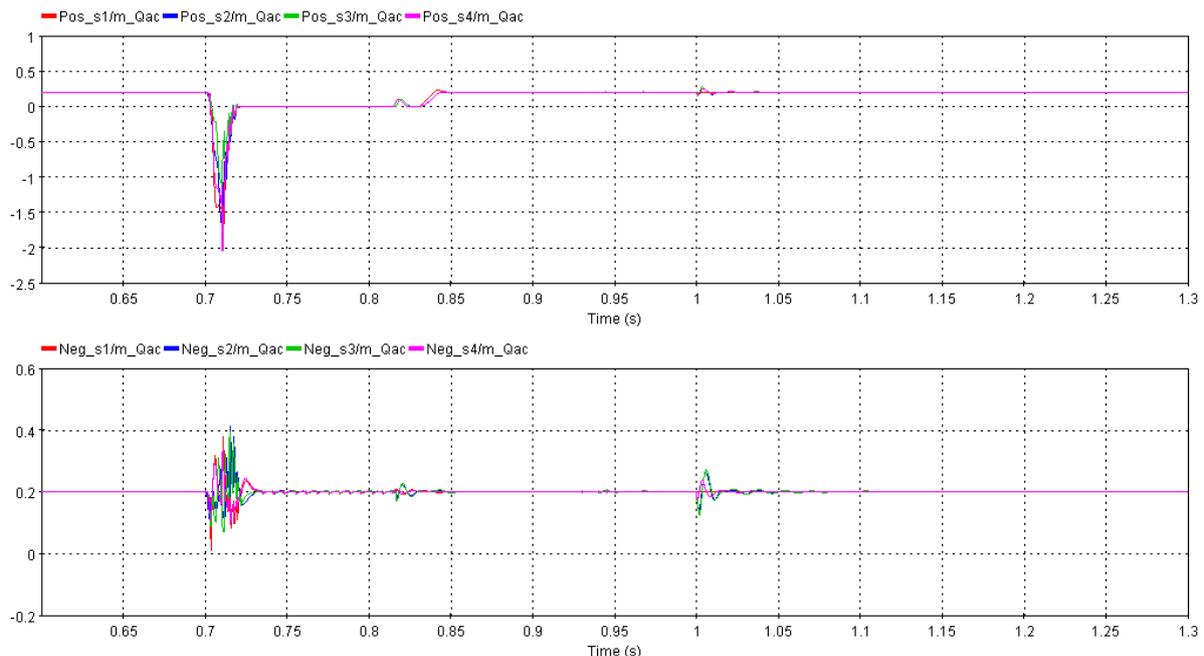
### D3.3: Protection Concepts

is caused by the restoration of DC voltage. The three remaining stations, S2, S3 and S4 bring power from their respective AC sides to reenergize the DC system, with their converters controlling the DC voltage to its reference value. This power transient is not seen in the s1 converter since it is in P-mode. Then, power is taken to its original reference values.



**FIGURE 2-11: ACTIVE POWER IN THE STATIONS OF THE MESHED DC GRID.**

The reactive power presents a similar behavior when compared with the active power, but the restoration of the faulty converters happens 130ms after the fault to operate as a STATCOM, which can be considered very fast to provide voltage support to the grid. The reactive power profile is presented in Figure 2-12.



**FIGURE 2-12: REACTIVE POWER IN THE STATIONS OF THE MESHED DC GRID.**

This subsection illustrates the DC FRT of the simplest hybrid system in terms of architecture. The objective and role of the C&P coordination and the sequence that should be followed once a fault occurs on the DC system when applying a non-selective protection strategy with DCCBs. The general and particular behavior of the system along this process has been described identifying and corroborating the expected behavior of each of the elements involved. This study case then serves as a reference of the DC FRT for a hybrid system.

## 2.2. Weak Grid Scenario

In this section, the SCR of the grid is adjusted to  $SCR=1.9$  to configure a grid model with diminished strength, which can be considered a very weak grid ( $SCR < 2$ ). This alteration results in an increase in the equivalent impedance between the grid source and the converter, thereby diminishing the system's capacity to transfer power. Consequently, challenges arise in the PLL control and inner current loop control. The focus of the analysis in this context is on the system's response during a DC fault, specifically emphasizing the DC-FRT capability.

As in the previous case, the four stations are in bipolar configuration, station 1 is operating in P-mode control, while the rest are performing Vdc control with the same droop, consequently the three remaining stations share in the same proportion the DC voltage control. The C&P coordination leads to the same simulation sequence as in the first use case, which is here repeated for convenience. The given sequence is expected to highlight differences between each of the control strategies. At the same time, their advantages and disadvantages will be illustrated, such as the voltage stiffness handling capacity by each of the controls.

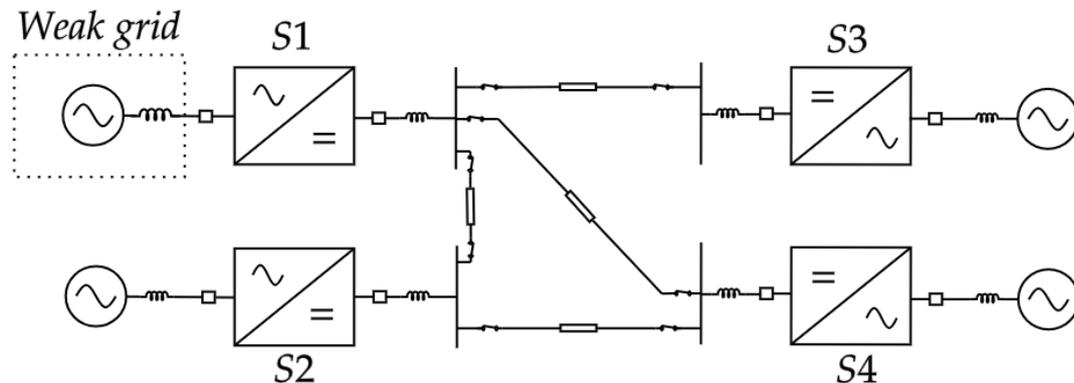
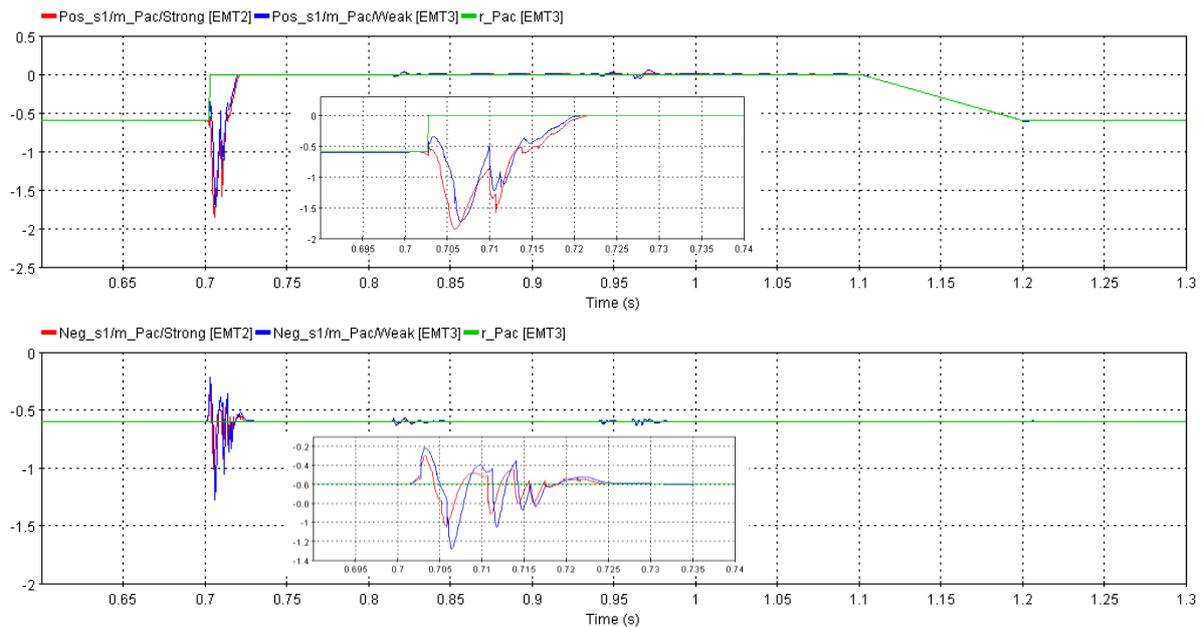


FIGURE 2-13: ELECTRICAL MODEL OF STRONG GRID CONNECTED TO THE MESHED MTDC GRID.

The low voltage stiffness will impose difficulties to the GFL control since any power variation will imply a considerable change in voltage. Thus, the PLL control have a major influence on system dynamics, requiring an adjustment on the PLL dynamics to properly track the grid phase. Figure 2-14 introduces the comparison of active power between strong (in red) and weak grid (in blue). It is evident that the active power of Pos\_S1 and Neg\_S1 undergoes notable changes when compared with strong grid scenario. Power peaks are reduced for the weak grid, and the time response becomes slower compared to the scenario with a strong grid. The faulty pole Neg\_S1 exhibits increased oscillations after the reclosing of the DCCB in comparison to the simulation in a strong grid environment.



**FIGURE 2-14: COMPARISON OF ACTIVE POWER PROFILE BETWEEN STRONG AND WEAK GRID.**

In this instance, the characteristics of the weak grid are once again evident through the reactive power behavior outlined in Figure 2-15. Notably, there is a reduction in reactive power peaks when compared to the strong network. However, it is noteworthy that the AC voltage variations depicted in Figure 2-16 for the weak network are considerably higher. In weak grids the requested reactive support is significantly larger in order to maintain a required voltage. In this specific scenario, the voltage drop is approximately 0.65 pu, which is approximately 0.2 pu higher than the observed in the strong network.

A closer examination of the voltage accentuates a more pronounced voltage transient, characterized by increased oscillations in this weakened network. The healthy pole has larger magnitude oscillations on the reactive power before the fault clearing, while the faulted pole reaches the same first peak as the strong grid, nevertheless, the lower voltage stiffness leads to faster oscillations and brings up the reactive power profile, having a smaller second peak in comparison with the strong grid. Going further in time, the restoration of reactive power pushes the AC voltage at the PCC towards a higher value, but still, this increase is not as smooth as the strong grid reference.

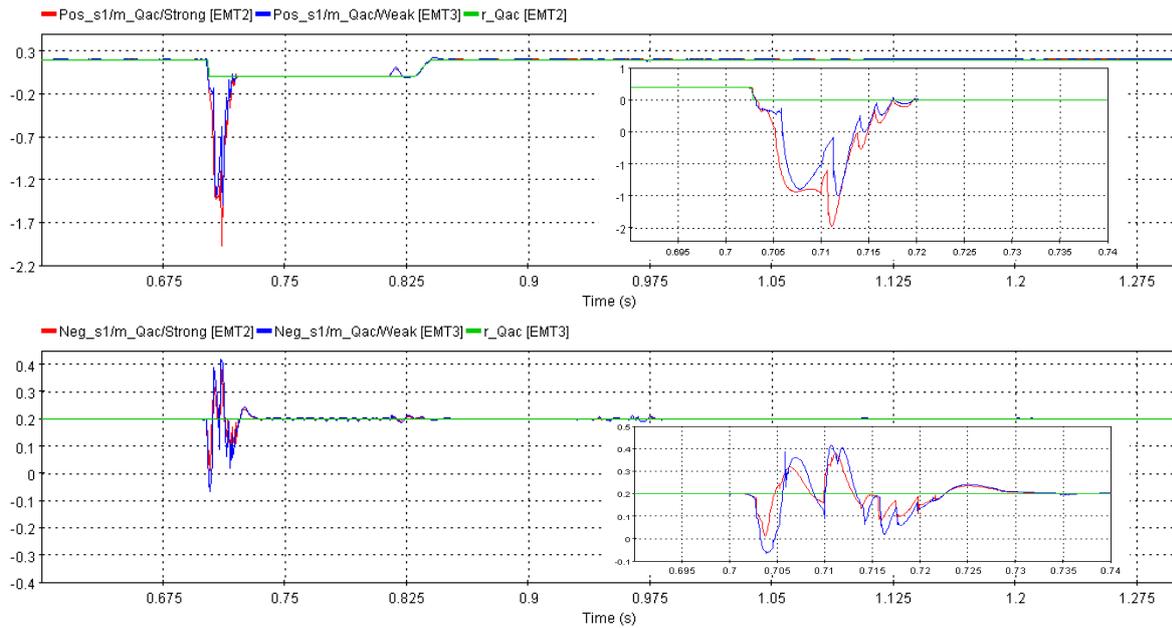


FIGURE 2-15: COMPARISON OF REACTIVE POWER PROFILE BETWEEN STRONG AND WEAK GRID.

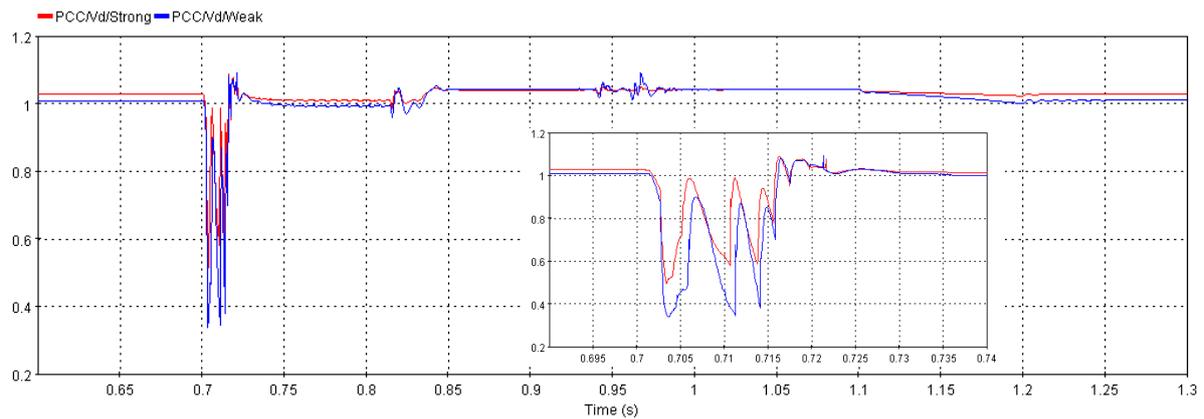
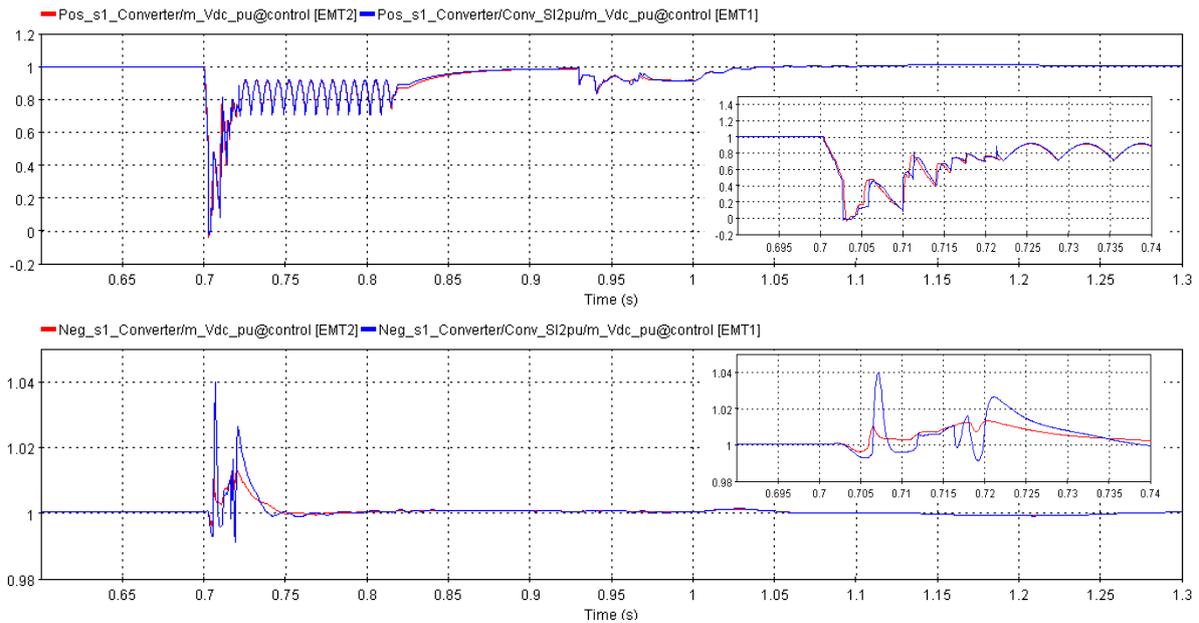


FIGURE 2-16: AC VOLTAGE MAGNITUDE AT THE PCC, STRONG AND WEAK GRID COMPARISON.

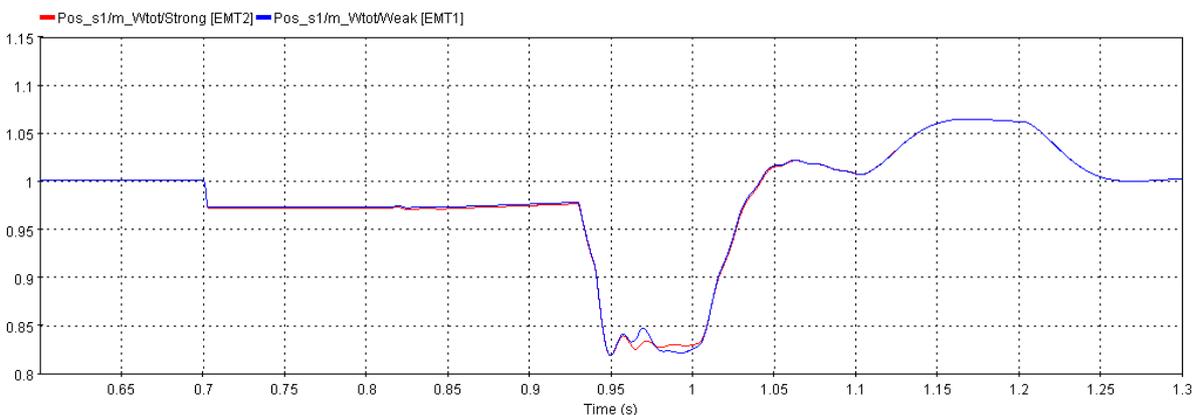
The DC voltages on the Pos\_S1 and Neg\_S1 poles are depicted in Figure 2-17. DC voltage has a similar behaviour as the one seen in the strong grid; nevertheless, the oscillations in the healthy pole are larger, as an expected consequence of the low voltage stiffness of the weak grid, requiring more power effort from the DC side. The faulty pole follows the FRT behaviour seen before, while the AC voltage magnitude has a brief voltage dip that is quickly recovered, and no major concern regarding its stability is identified. Both DC voltages, although with higher oscillations than those of the strong grid, remain stable for the whole DC FRT.



**FIGURE 2-17: DC VOLTAGE AT THE POSITIVE AND NEGATIVE POLES, STRONG AND WEAK GRID COMPARISON.**

The control of internal energy within the converters is managed by the DC side of the converter, specifically by regulating the energy stored in the capacitors within the converter submodules. Consequently, when the DC voltage is effectively controlled, the internal energy is appropriately managed. However, in the case of station S1 operating in P-mode, the internal energy remains unregulated during the period when the DC side of the grid is disconnected, spanning from the MMC deblocking to the reclosing of the DCCB.

The behaviour of internal energy in the faulty pole (Pos\_S1) is illustrated in Figure 2-18, showcasing uncontrolled internal energy fluctuations between 0.815s and 0.930s of simulation time. Subsequently, with the restoration of the DC side, stability is restored as the internal energy stabilizes at the desired level. Although this minor variation in internal energy may not pose a significant issue for the GFL control, it could potentially present challenges for GFM control due to its dependence on the frequency-power relationship. Therefore, a comprehensive analysis within the GFM control scenario is warranted to evaluate and address any potential stability concerns arising from these internal energy fluctuations.



**FIGURE 2-18: TOTAL ENERGY IN THE FAULTY POLE (POS\_S1).**

## 2.2.1. GFM Control Implementation

The virtual synchronous machine (VSM) is implemented in this section, following the definition presented in (1). Special attention will be set on the energy levels of the faulted converter when performing GFM control, since this type of control has an active response to the AC side conditions and will introduce electromechanics dynamics to the AC side due the emulation of a synchronous machine.

The weak grid case with grid-forming control implemented is expected to have a better response in terms of voltage and frequency dynamics, since now the converter is acting as a voltage source creating the voltage signal at the AC connection and sharing the AC system stability with the main grid. Therefore, the GFM converter will react to AC system perturbations, providing active power for frequency excursions and reactive power for AC voltage variations, resulting in an overall reduced impact in AC system stability responding to a DC fault. Consequently, GFM control strategy will enhance the voltage and frequency stability of weak grids.

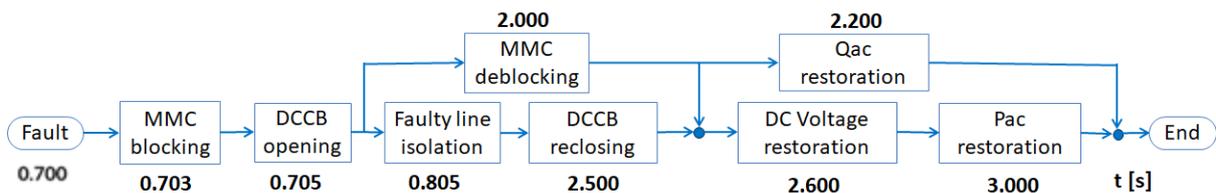
The above-described response is a real advantage of the GFM control. Nevertheless, in GFM control, the perturbations of the AC grid are propagated to the DC side of the grid, resulting in higher impacts to DC side, increasing the control effort of the whole AC/DC system. Once the DC side is absorbing the perturbations from the AC grid, the other stations (S2, S3 and S4) will also transmit these perturbations to the respective AC grid they are connected to, which implies, at the same time, perturbation propagation and sharing the control among the stations to mitigate the perturbations in the GFM station. In conclusion, this characterization is going to be detailed to define the behaviour of the AC/DC system when the station S1 is in GFM control.

From an operational standpoint, it is expected that the settling time significantly increases in comparison to the case of GFL control. This prolonged settling time is attributed to the slower response of the Virtual Synchronous Machine (VSM), characterized by a bandwidth of 0.5Hz (with VSM parameters defined as:  $H = 2s$  and  $D_p = 80$ ). Consequently, adjustments are required in the inner loop control (voltage and current) of the GFM converter to align with the external power control loop. While this adaptation diminishes the likelihood of oscillatory behaviour due to control interactions, simultaneously it substantially reduces the time response compared to GFL control (from 100ms to 2s). The transfer function relating the power angle and power reference is presented next, where the natural frequency and the damping term can be extracted:

$$\frac{\delta(s)}{P^*(s)} = \frac{\omega_n}{2Hs^2 + D_p s + \omega_n P_{max}} \tag{2.3}$$

where  $\omega_n$  is the nominal angular speed and  $P_{max} = E \cdot V / X_{eq}$  is the synchronizing power coefficient.

In light of these adjustments, it becomes imperative to adapt the protection sequence to comprehensively evaluate the behaviour of GFM control under DC FRT conditions. The expanded version of the protection sequence is depicted in Figure 2-19, wherein the time-scale of the temporary loss is extended to analyse the performance of GFM control. Specifically, the temporary loss duration is increased from 400ms to 2.3s, a modification implemented solely for investigative purposes rather than reflecting real-time sequences.



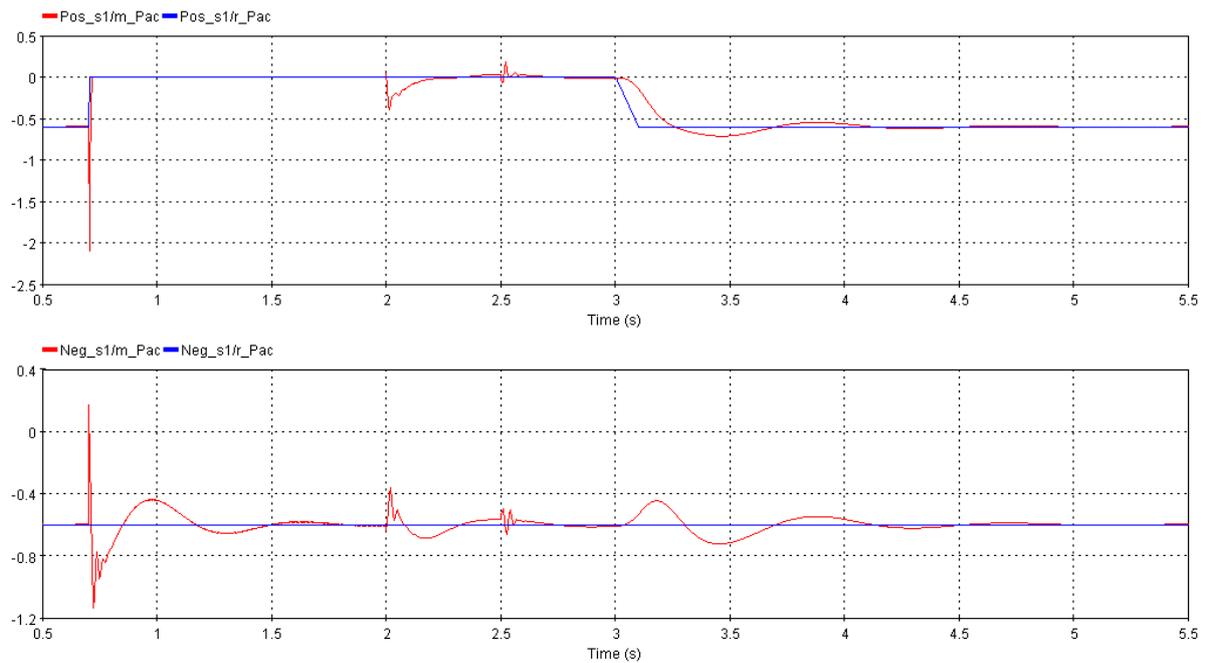
**FIGURE 2-19: ADJUSTED TIME-SCALE PROTECTION SEQUENCE FOR GFM CONTROL.**

Figure 2-20 depicts the active power profile when the converters of station S1 are in GFM control. It is clear that the speed dynamics of the active power are much slower compared with GFL control, taking few seconds to reach the steady state after a power perturbation. On the faulted pole, the power peak is driven by the fault current, injecting a high peak of power to the DC grid until the DCCB is opened, then taking the power to zero. With this control strategy, the fault current rises the power peak up to 2.1 pu.

On the other hand, the healthy pole Neg\_S1 initially reacts in opposite direction of the fault current, providing power to support the AC grid, which reduces the power imbalance impact in this event thanks to the virtual inertial response of the VSM. This is a great advantage of the GFM control strategy, where the converter behaves as a synchronous machine improving the AC grid stability. Nevertheless, the initial power peak of the healthy converter comes from the DC grid, which means that the perturbation is now propagated also to the DC side of the grid by the healthy pole. But the perturbation on the DC grid is not impacting the stability of the system as is going to be shown in the DC voltage figure. After that initial power imbalance response at the first moment of the fault, the second part of the disturbance progress comes with the breaker opening, which leads to the fault current extinction and loss of the power flow on the faulted converter, seen as a loss of load at the PCC, which changes the voltage angle at the PCC and the healthy converter perceives this as a phase jump that leads to a power transient response that absorbs a larger amount of power from the AC side. The healthy converter reacts to the phase jump seen in the point connection between the positive pole and the grid, since the faulty pole angle had an abrupt change taking the power supply to zero. Nevertheless, the healthy pole responds injecting power to the DC grid until a new equilibrium point is achieved, bringing Neg\_S1 back to its power reference, the stabilization time of the new equilibrium point is just over 1 s.

Once the fault is isolated, the faulty converter is deblocked at 2 s of simulation, which result in a small transient of power for both converters caused by the mismatch of the initial phase of the faulty converter when the swing equation is reactivated (swing equation is reset at the same time the MMC is deblocked). In this case, it need to be highlighted that the initial value for reset of the swing equation is extremely important to do not generate any phase mismatch, which will cause power transients in the system, therefore, the initial value of the power angle for the swing equation can be set as the same measured value of the PLL angle, where no power mismatch is resulted applying this value.

The DCCB is reclosed at 2.5s of simulation, therefore the DC side of the grid is now available to perform the power exchange between AC and DC side, control of the faulty converter's internal energy is resumed. At 2.6s the DC voltage is restored, which does not cause any disturbance in station 1, since it is in P-mode. And finally, at 3.0 s of simulation the active power is restored and the power returns to its original value before the fault according to the VSM dynamics. It is worth noting that any power perturbation in one pole is now reflected to the other pole because of the characteristics of the VSM strategy, with has an intrinsic inertial response.



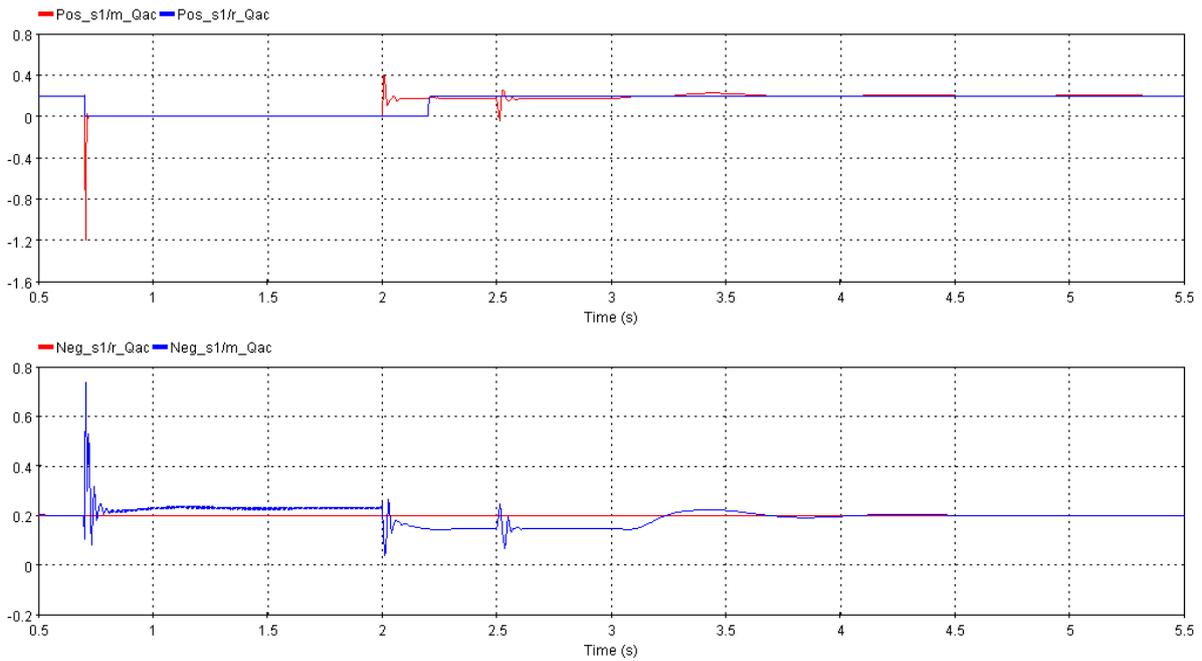
**FIGURE 2-20: ACTIVE POWER PROFILE OF STATION S1 IN GFM CONTROL.**

The reactive power and its reference for station 1 is presented in Figure 2-21. The control of reactive power is coupled to the AC voltage generation via droop control. Thus, the reactive power support will be retaken once the faulty converter is deblocked. The reactive power droop control has an inherent voltage regulation action, where following the reactive power reference does not represent a priority, so when the faulty pole is deblocked, the converter's voltage control is activated, supplying the required amount of reactive power to regulate the AC voltage. The AC voltage control is shared through the droop control between the poles, so the healthy converter also shifts its value of reactive power supply to share it with the faulty converter, obtaining a new equilibrium point. Once the active power is restored, the system reaches the original pre-fault equilibrium point, and then the reactive power is able to follow its reference for the given operating point.

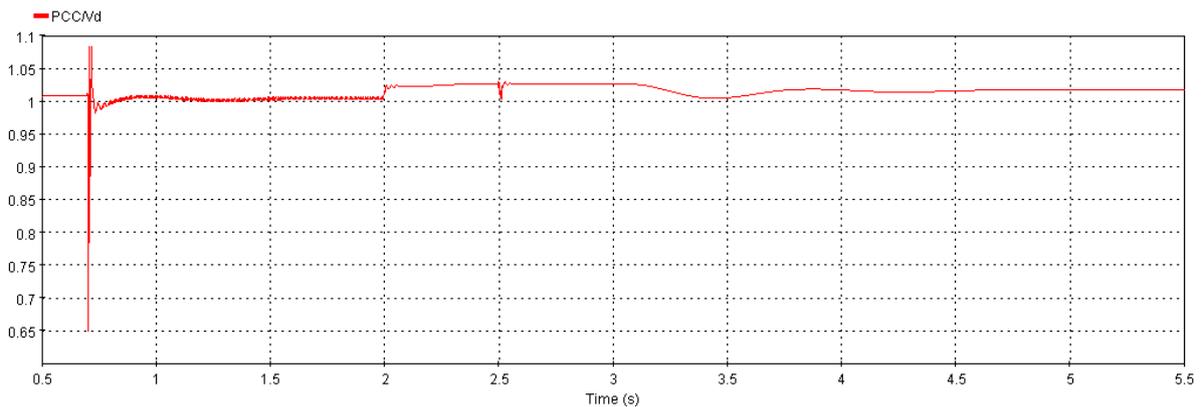
AC voltage magnitude profile for the DC-FRT is depicted in Figure 2-21. It presents a huge drop during the first part of the short circuit transient and rapidly recovers once the DCCB is opened. A zoom on the AC voltage magnitude and three-phase waveform is portrayed in Figure 2-23, which shows a voltage drop to 0.65 pu during the fault. It can be highlighted here that the impact on the AC voltage is strongly reduced when compared with the GFL control (where the AC voltage sags below 0.4 pu). The voltage sinusoidal waveform has a small distortion during the fault disturbance, but that does not represent any issue to voltage stability. Therefore, no concern in terms of voltage stability is identified with the implementation of GFM control strategy, and indeed, this control strategy enhances the weak grid behavior at the PCC, as expected since there converters are sharing the responsibility of maintaining the AC voltage.

As of the deblocking of the faulted converter, the AC voltage level on the PCC increases due to the reactive power injection of the faulty pole and the reduced power flow at the point of connection, while the operating point stabilizes close to 1.02 pu. It is until the pre-fault power flow is recovered that the voltage level reaches its nominal value with a large settling time derived from the VSM slow dynamics.

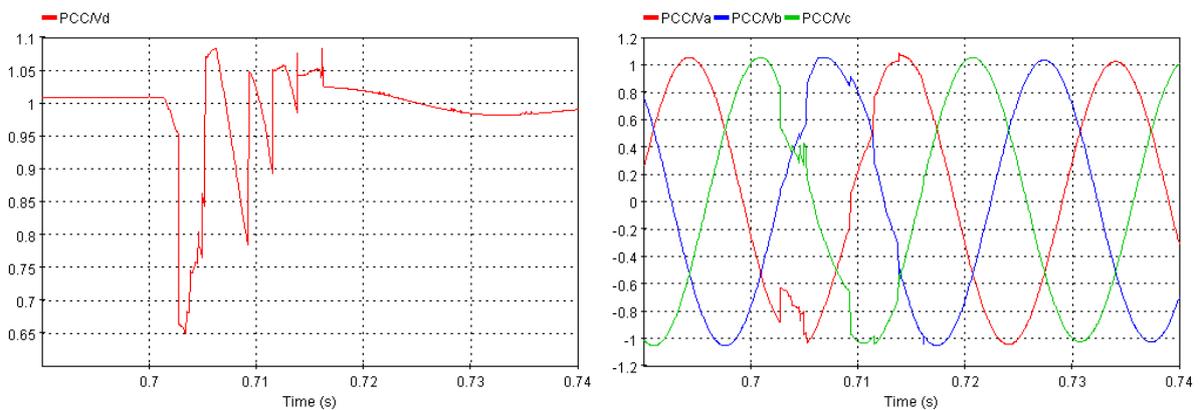
### D3.3: Protection Concepts



**FIGURE 2-21: REACTIVE POWER PROFILE OF STATION S1 IN GFM CONTROL.**



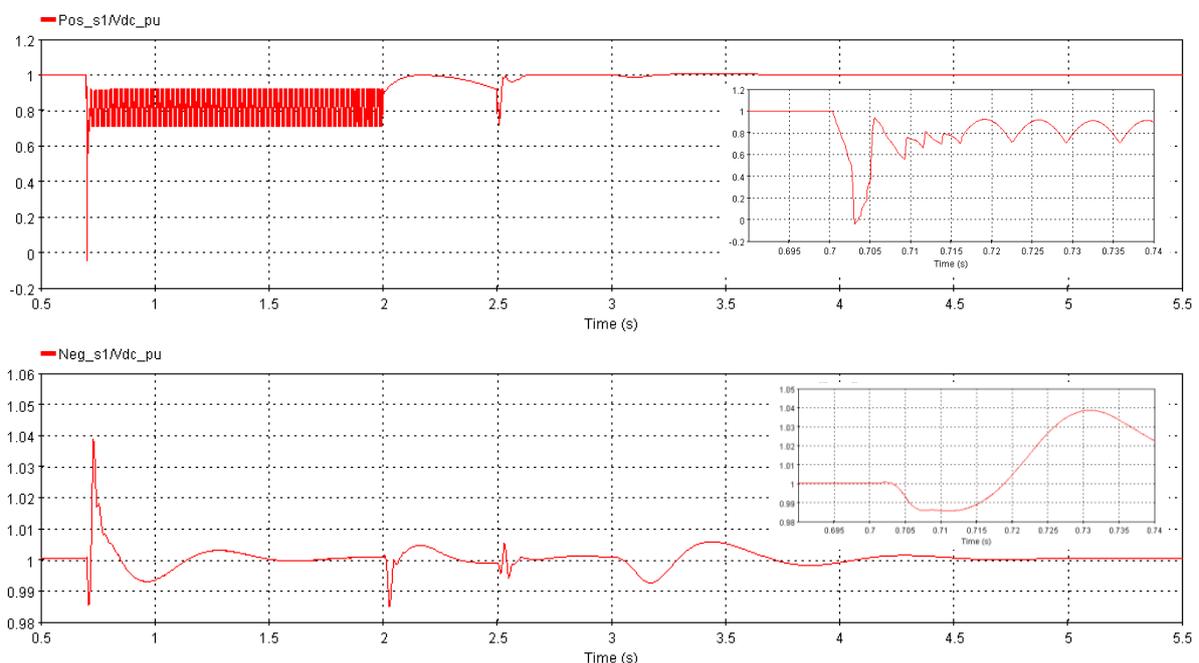
**FIGURE 2-22: THE AC VOLTAGE MAGNITUDE AT THE PCC.**



**FIGURE 2-23: THE AC VOLTAGE MAGNITUDE AND THREE-PHASE WAVEFORM ZOOM DURING FAULT TRANSIENT.**

Figure 2-24 depicts DC voltage at the station 1 of the MTDC and the protection parameters are presented in Table 2-6. The faulted pole has the expected profile seen in previous analyses, yet this

time the DC voltage varies in a non-controlled manner when the faulty converter is deblocked, indeed internal energy of the converter is not controlled during this period until the DCCB is reclosed, therefore, the DC voltage also is not properly controlled during this event. Once the DCCB is reclosed, DC voltage is then controlled to its nominal value after a mild transient due to the internal energy control asking for power to charge the submodule capacitors. The DC voltage on the healthy pole has a perturbation due to the power transient response of the VSM converter, first small dip given by the power imbalance on the grid and later a brief increase due to the reaction to the phase jump seen by the healthy converter. This perturbation seen in the DC voltage indicates the propagation of perturbation from the AC grid side response of the GFM control, originally given by the DC fault on the positive pole. This perturbation is now coming from the positive pole to the negative pole, which generates a reaction of the DC voltage control shared by the other 3 stations (S2, S3 and S4) responsible for DC voltage stability. This perturbation will be later seen as a power response for S1, S2 and S3 stations in the AC side.



**FIGURE 2-24: DC VOLTAGE AT THE POSITIVE AND NEGATIVE POLES.**

The DC voltage behavior encountered in the faulted pole is also reflected in the internal energy of the converter. The internal energy increases its value beyond the actions of the control from the DC side of the grid, since no possibility to evacuate power from the DC is available. Thus, the energy control is not capable of correcting the actions taken by the VSM and an overcharging of the converter capacitors occurs. The internal energy is depicted in Figure 2-25, where the blocking of the converter is clearly identified after the fault freezing the energy control during this time. Once the MMC is deblocked, the internal energy increases and it is only when the DC side is reconnected that the converter can evacuate power and restore the energy level to its nominal value. The submodule capacitors overcharging level reached beyond 1.6 pu for nearly 200 ms. It is evident here that this operating condition can cause instability, since this perturbation will require a response that the control blocks related to DC voltage and internal energy control are not prepared to deal with. So, the internal energy and DC voltage controllers are limited in their time of response and cannot provide the correct action in this situation, which may cause instability even for small periods of time, since the energy increases quickly to unsafe values. Therefore, alternative control actions should be taken. Two control alternatives are here proposed to mitigate this issue: first is to implement an outer energy

control loop controlling the energy from the AC side of the grid, and the second is to change control from GFM to GFL during part of the FRT operation. With this alternative control action, a soft restoration is expected which would avoid the overcharging of the submodule's capacitors.

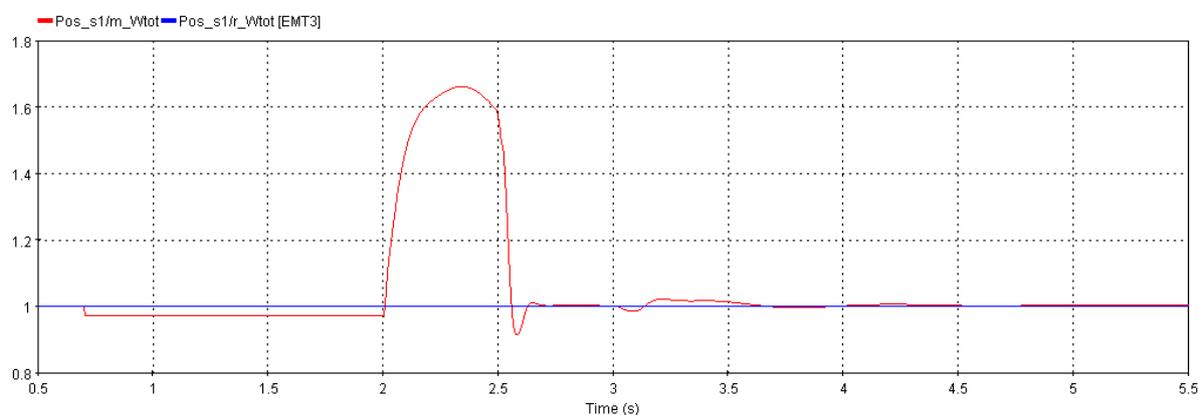


FIGURE 2-25: INTERNAL ENERGY OF THE POSITIVE POLE IN STATION 1.

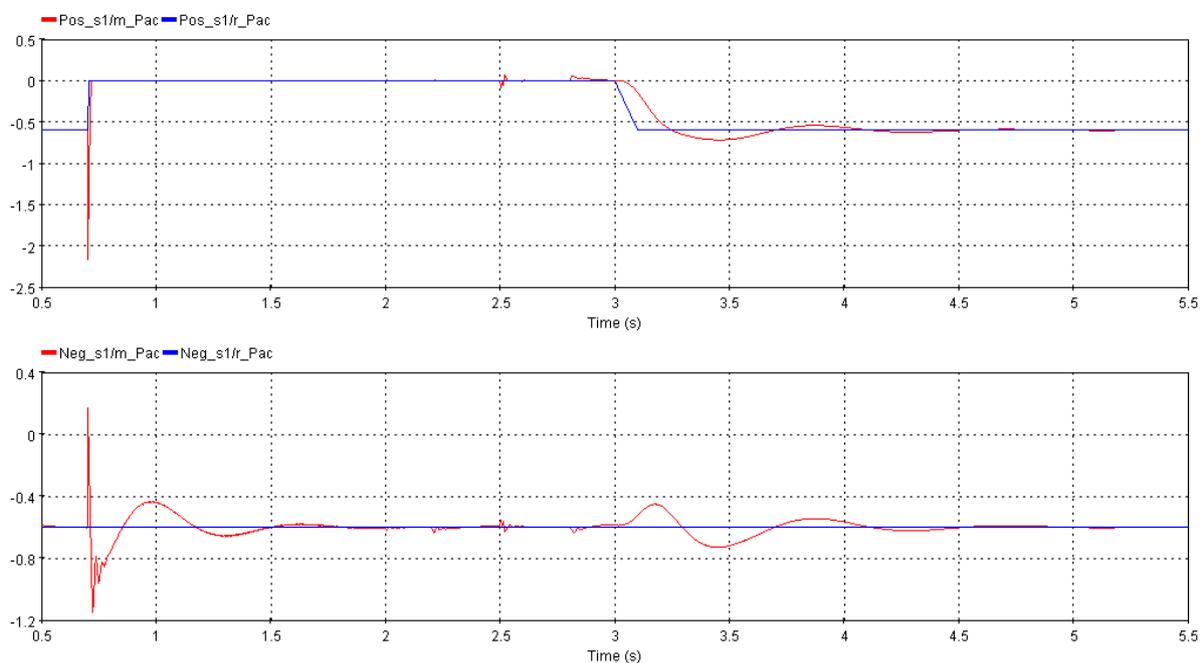
### Proposition: DC-FRT from GFM to GFL

In this section it is proposed to switch from GFM to GFL during the DC FRT operation, i. e., in a presence of a DC fault, after the MMC blocking, the control strategy shifts to GFL to avoid the identified impacts of GFM during the DC FRT period and retake GFM control after the DC voltage restoration. The main purpose of this approach is to eliminate the internal energy control problem evidenced in previous analysis, which could cause damage to the converter submodules. Furthermore, as the GFL control have fast dynamics characteristics together with smooth transients during the FRT, this approach is expected to avoid the slow power transients at the station under analysis and to have a soft restoration process with the same time of temporary loss as for GFL (400 ms). The implementation to switch the control from GFM to GFL is made by changing the voltage modulation indexes (PWM input) from voltage control loop to the current control loop keeping the power references as the same for both controllers, therefore, the converters is now behaving as a current source, following the phase angle provided by the PLL. Next, to switch from GFL to GFM it is implemented a smooth transition, where the measured voltage on the AC grid is taken as the initial reference for the GFM voltage control, avoiding high power transients to follow the new control reference, where in this case the voltage source behavior is now reactivated in the converter. More details on this approach can be found in [28, 29].

The proposed sequence to perform this alternative control action is presented in Figure 2-19. In this case, the GFM is shifted to GFL at the moment the MMC is deblocked, being in GFL during the whole DC FRT operation, and the control is shifted back to GFM control 200 ms after the DC voltage is restored in the MTDC, i. e. at 2.8 s of simulation. Therefore, the active power can be properly restored already considering the GFM feature, which has the inherent inertial support. The idea here is to illustrate the switch back to GFM control without any other mutual control action to explicitly analyze the behavior of this strategy. In summary, the proposed action (from GFM to GFL) avoids power transients during the deblocking of the converter and at the same time allows the internal energy level of the faulty converter to remain under safe margins.

Figure 2-26 depicts the active power profile of the proposal switching from GFM to GFL control. The behavior of the faulty converter is quite similar to the previous cases in the first moment of the DC fault, but when the converter is deblocked, the control is shifted to GFL minimizing the power

transients for both converters (faulty and healthy converters). This is because the voltage control is not reactivated in the faulty converter and the control reference remains at zero, so no disturbances are generated by the faulty converter, not propagating any disturbances to the healthy converter either. Once, the DCCB is reclosed and the DC voltage restoration is performed, the shift from GFL to GFM control is done, considering the smooth transition, both the AC voltage magnitude and the grid angle calculated by the PLL is applied to the voltage droop control and to the swing equation, respectively, in order to obtain a seamless transition to GFM control. Furthermore, in order to switch back to GFM control, a resynchronization of the VSM frequency and angle is done, permitting another smooth transition. The last control action, retaking active power set point is performed with the VSM response (which can be seen by the slower dynamics at 3 s of simulation), which provides frequency support to the AC grid. The healthy pole (Neg\_S1) remains in GFM mode during the whole time of simulation, it can be seen that the perturbations in between the deblocking of the converter and the restoration of active power are minimal, which can be concluded as a smooth DC FRT operation.



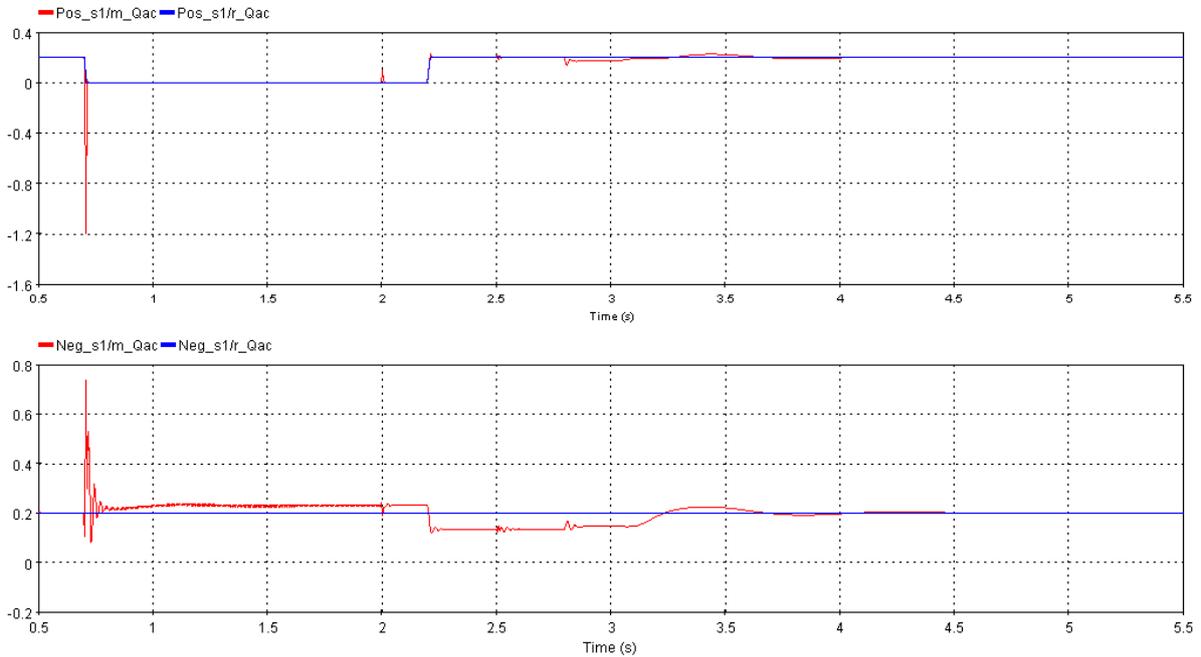
**FIGURE 2-26: ACTIVE POWER PROFILE IN STATION 1, CONSIDERING GFM TO GFL PROPOSAL.**

In the case of reactive power, the profile of the faulty pole Pos\_S1 has a smoother operation when compared with the GFM control, since it is following the GFL dynamics, once the reactive power is restored, the faulty pole can regulate reactive power back to its reference value, while the healthy pole provides the voltage support according to the voltage droop control, which seems to have a softer reaction to reactive power. Nevertheless, during this period, only the healthy pole is providing AC voltage support to the grid which is adapted according to the faulty pole reactive power supply, while the faulty pole is only providing reactive power according to a reference. The reactive power of station 1 is depicted in Figure 2-29, according to the GFM to GFL control transition.

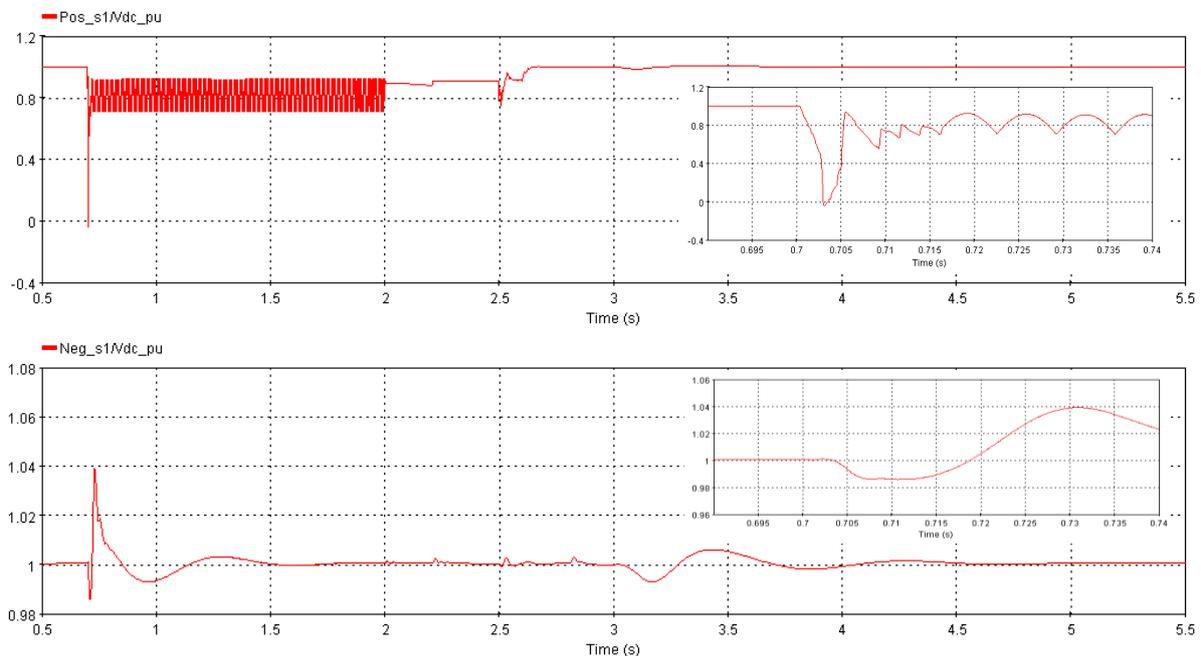
The DC voltage on station 1 of the GFM to GFL control proposition is depicted in Figure 2-28. Both the faulty and healthy converters present same initial behavior considering GFM control as expected, but during switch of the faulty pole to GFL control, the DC voltages present smaller spikes, being less affected in this case. Therefore, it can be concluded that the DC side of the grid is not really impacted considering GFL control (no action to AC grid dynamics), and the perturbation of the AC are not propagated to the DC as in GFM control, which can be considered a good solution if the DC system is

### D3.3: Protection Concepts

meant to not react to AC disturbances. From the other point of view, it means that the impacts on the AC side can be considered only supported by the healthy converter. At 2.6 s the DC voltage control is restored by the other stations and then the DC voltage on both poles of station 1 are controlled in its reference, the next relevant transient refers to the active power restoration.



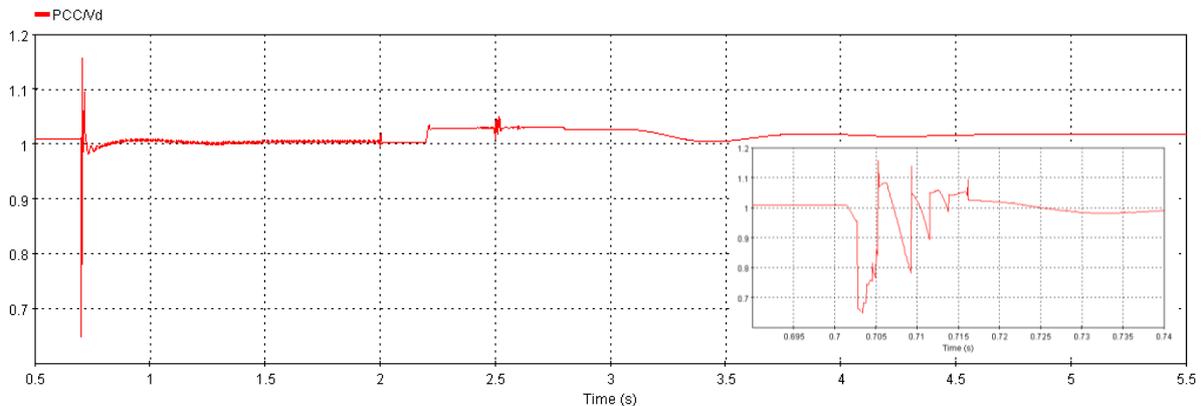
**FIGURE 2-27: REACTIVE POWER PROFILE IN STATION 1, CONSIDERING GFM TO GFL PROPOSAL.**



**FIGURE 2-28: DC VOLTAGE IN STATION 1, CONSIDERING GFM TO GFL PROPOSAL.**

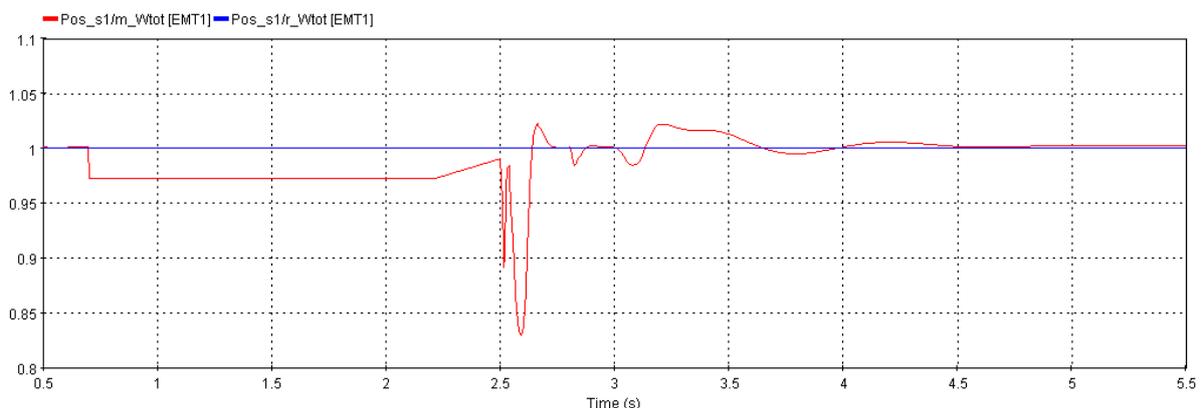
The AC voltage on the PCC has a direct relation with the reactive power supply on the AC side of the grid, therefore its magnitude is slightly changed when switching to GFL control in comparison with the GFM control approach, since the converter now is deblocked but no control action towards the AC voltage is taken by the faulty converter until the reactive power is restored. When the reactive power

is restored in the faulty pole, the voltage rises to a new equilibrium point, and the healthy pole reacts reducing the reactive power supply to aiming to regulate the voltage. Therefore, when the active power is restored, the system is back to the original equilibrium point with the faulty converter also switched back to GFM control. The reclosing of the faulted pole DCCB is identified with fast oscillations due to fast power transient. The AC voltage on the PCC is depicted in Figure 2-29.



**FIGURE 2-29: AC VOLTAGE MAGNITUDE IN THE PCC, CONSIDERING GFM TO GFL PROPOSAL.**

The internal energy of the faulty pole is introduced in Figure 2-30, which shows how the internal energy behaves during the DC-FRT when considering the shift from GFM to GFL control. One of the aims of the GFM to GFL proposition is to maintain the energy level of the faulty pole under safe margins, which can be achieved by removing the reactive power control effort of the AC voltage droop control towards the capacitors of the submodules. Since the internal energy is controlled by the DC side of the grid, during the fault, DC side is not available to compensate power to regulate the internal energy of the MMC requested to perform voltage control. In GFL control mode, there is no voltage control, therefore, the internal energy is kept constant until the reactive power is restored, which starts to change in a low-rate profile. This does not represent an issue for internal energy control, unless the STATCOM operation mode is kept in long term. In long term operation of STATCOM mode, it would be necessary to have the converter operating in Vdc-mode, so that the internal energy is compensated according to the required energy in the submodule’s capacitors.



**FIGURE 2-30: POSITIVE POLE CONVERTER TOTAL ENERGY.**

Nevertheless, in the GFM to GFL proposition, the power surge is not present during the deblocking of the faulted pole converter thanks to the inherent behavior of GFL control. The internal energy level of the faulted converter has a very low rate of change once it is deblocked, which does not affect the variation of energy in the capacitors submodule in a significant way to cause instability issues. After

the reclosing of the DCCB, the connection of the DC side allows the regulation of the internal energy by the stations in Vdc-mode, then at 2.6 s in the simulation the DC voltage restoration is activated, which properly control the energy in its reference.

It is important to highlight that this is an extended control sequence, thus in reality this sequence would be completed within 400ms of temporary loss of infeed, reducing even further the possible control issues of the internal energy controllers for the capacitor’s submodule.

**Proposition: DC-FRT in GFM control (with outer energy control loop)**

The second proposed control alternative is to keep the GFM control during the whole DC-FRT operation, where an outer energy control loop is implemented to provide an active power reference to the VSM control, such that the internal energy is controlled by the AC side of the grid while the DC side is not available. The power reference produced by the outer energy control loop is added as the power reference for the faulty pole during the fault. The block diagram of the internal energy controlled by the AC side of the grid is introduced in Figure 2-31.

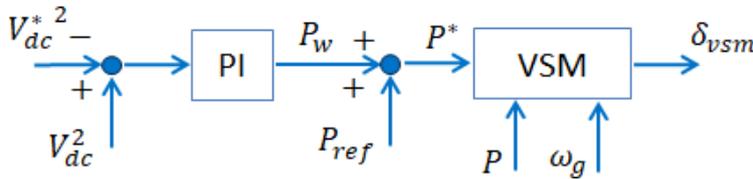


FIGURE 2-31: BLOCK DIAGRAM OF THE OUTER ENERGY CONTROL LOOP.

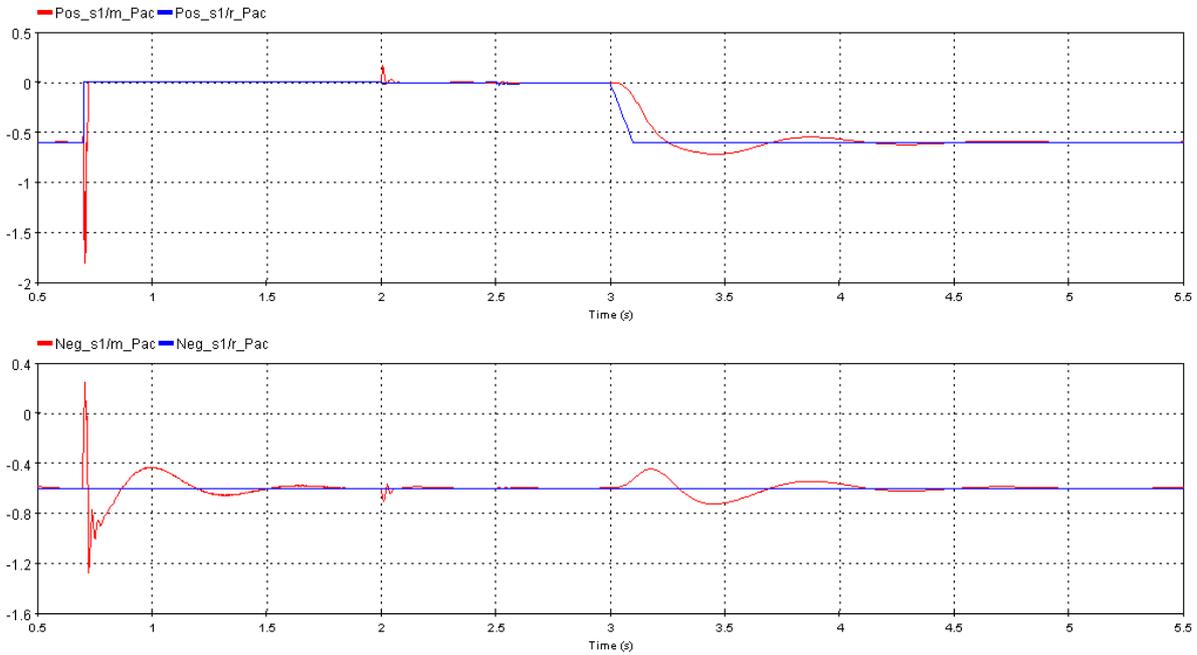
The internal energy variation is given by  $V_{dc}^2 - V_{dc}^{*2}$ , which is controlled by a PI controller. The DC voltage reference is given by  $V_{dc} = 1 pu$ ,  $P_{ref}$  is the original reference given by the station control (during the fault the power reference is zero),  $P_w$  is the output power from the energy control, calculated such that the energy is controlled in its reference.  $P^*$  is the resulted power reference that is applied to the virtual swing equation of the converter. This strategy is only applied to the faulty pole.

The PI controlled in tuned such that, a time constant of  $T_s = 2s$  is obtained for the internal energy dynamics, the damping coefficient is  $\zeta = \sqrt{2}$ . The gains of the PI controller are given  $K_p = 0.085$  and  $K_i = 0.09$ . The tuning of the PI controller is done considering the VSM dynamics, which has a time constant of 1s. Thus, the outer control loop has slower time scale dynamics to the proper performance of this cascaded control structure.

The deblocking of the converter can be seen as the reactivation of the VSM strategy in the faulty pole. Therefore, after the MMC deblocking, the control of the AC voltage is retaken and a transient of power can be seen. To minimize the perturbation in the system, the swing equation and the AC voltage control must be properly reset using the measured PLL angle from the AC grid and the AC measured voltage magnitude as the initial condition values, respectively. This results in an initial state of zero power reaction from the faulty converter, smoothing the deblocking procedure of the converter. One of the main advantages of this proposal is that the GFM response would be kept along the DC FRT and its inherent advantages, such as grid frequency and voltage support.

The power profile in station 1 for the DC-FRT in GFM with the external energy control loop is depicted in Figure 2-32. The power response during the deblocking transition turns to be smoother in comparison with the response that does not take any alternative action; only a small power transient occurs, which would not represent any hinder to the converter operation. The later control actions, reactive power, DC voltage control and active power restoration are done without major concern. On the other hand, the healthy pole converter active power profile reacts to each of the dynamic actions

done by the other converter. In general, this proposition presets smoother power transients for the faulty and also for the healthy converter, which means that less perturbation is induced during the DC FRT operation, representing an improvement for the system operation considering GFM control. The external energy loop minimally disturbs the active power reference, and it is going to be shown that the internal energy is controlled, which is also a great improvement.

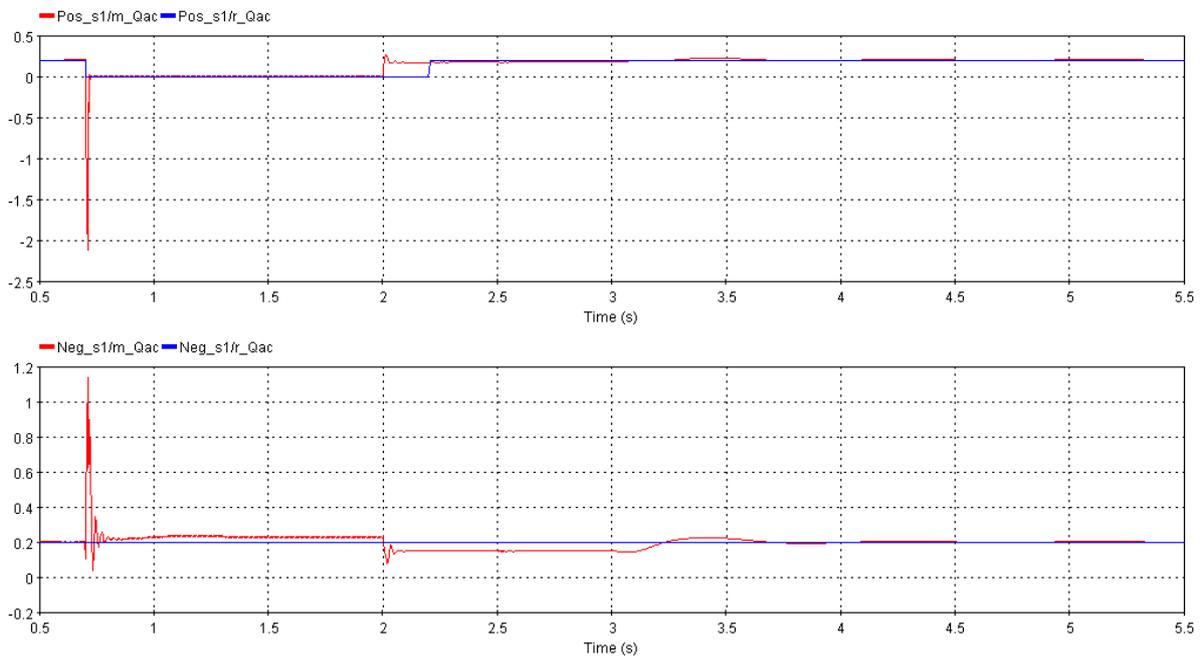


**FIGURE 2-32: ACTIVE POWER PROFILE IN STATION 1, CONSIDERING GFM WITH OUTER ENERGY CONTROL PROPOSAL.**

One of the main advantages of this alternative control action is illustrated with reactive power behavior, as depicted in Figure 2-33. The faulty pole begins STATCOM operation once deblocked without any activation signal needed. This is an inherent feature of GFM control to control the AC voltage from a droop control strategy, by injecting/absorbing a proper amount of reactive power with no need of reactive power reference. In this sense, the reactive power injection to the AC grid does not follow its reference in the faulted pole converter, even when the reactive power is restored, and the reference is retaken from zero at 2.2 s of simulation. In the meanwhile, the healthy pole converter reacts as in earlier reviewed cases.

On the DC side, the voltage has a rather soft DC FRT concerning the deblock of the MMC since the internal energy is now controlled, the voltage is also controlled to the desired reference. Therefore, the overshoots of DC voltage in between the MMC deblocking and the reclose of the DCCB are mitigated. The healthy pole has an overall smooth transition, the brief power disturbance occurring while the other converter deblocks has a minimum impact. The later power restoration reaches a similar impact on the healthy converter as in previous alternative sequence since in both cases the VSM response is used. The DC voltage in station 1 is introduced in Figure 2-34. The proposed GFM control for the DC FRT also bring advantages for the AC voltage, presenting smoother dynamics when compared to the other cases as depicted in Figure 2-35. It has a sudden increase due to the inherent STATCOM response of the VSM, but the reconnection of the DC side is barely noticeable. It can be seen a general improvement of the AC voltage profile since the voltage support is given by both poles during the DC FRT operation.

Regarding the internal energy of the faulty converter, the outer energy loop control is able to use the AC side of the grid, by taking the active power to control the internal energy of the faulty pole after the MMC is deblocked until the DCCB is reclosed. The internal energy of the faulty pole is depicted in Figure 2-36. The internal energy has a much smaller overshoot when compared with the case without energy control, with variations smaller than 10%, thus it is considered that the internal energy is kept within the expected margins. This corroborates the effectiveness of the proposed energy controller, which uses the AC side of the grid to maintain the converter operation inside of the boundaries. Once the DCCB is reclosed, the converter has a brief discharge is seen which is quickly compensated by the original energy control on using the DC side of the grid (the external energy control loop is deactivated) and restores the energy level to reach its objective. Along these transient events, the outer energy control reacts and maintains the converter energy under safe margins, resulting in a suitable solution for the GFM control in DC FRT operation.



**FIGURE 2-33: REACTIVE POWER PROFILE IN STATION 1, CONSIDERING GFM WITH OUTER ENERGY CONTROL PROPOSAL.**

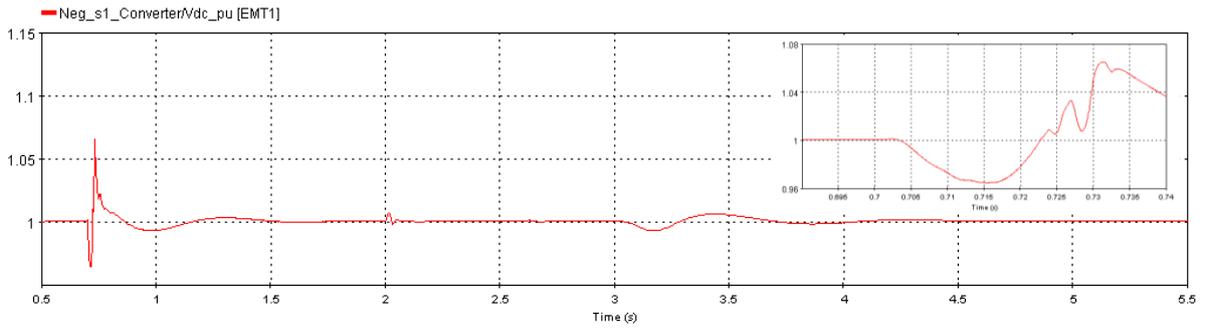
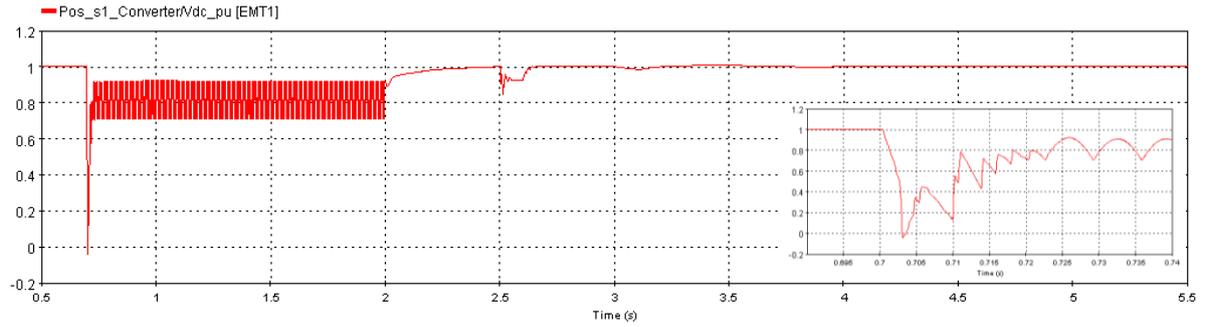


FIGURE 2-34: DC VOLTAGE AT THE POSITIVE AND NEGATIVE POLES.

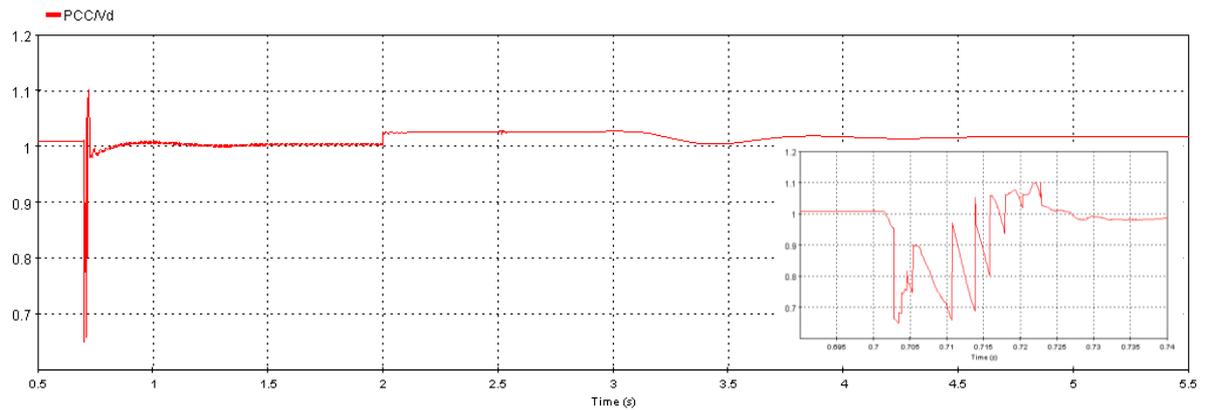


FIGURE 2-35: THE AC VOLTAGE MAGNITUDE AT THE PCC.

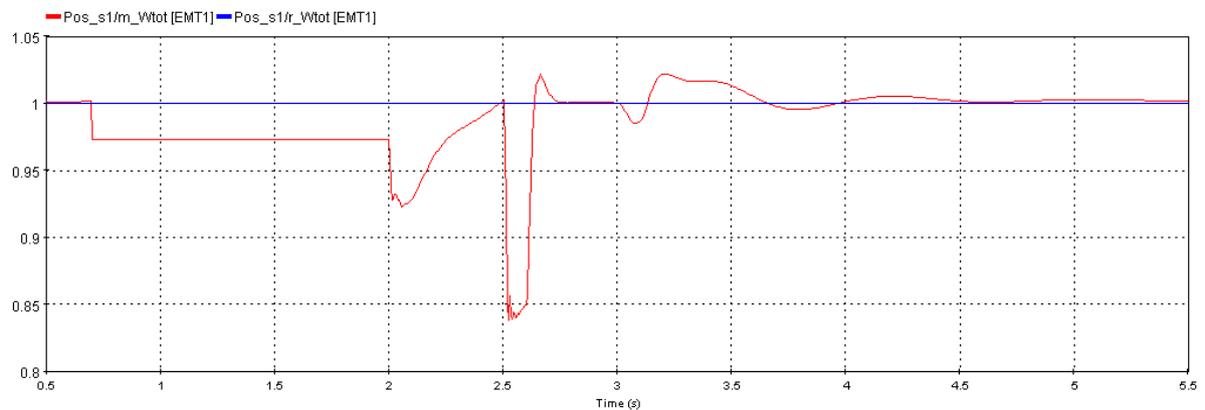


FIGURE 2-36: POSITIVE POLE CONVERTER TOTAL ENERGY.

## 2.2.2. Operational limits (Current limitation)

Further investigations considering the operation limits of the bipolar is carried out in this subsection. In this case the power flow is shifted to close to the nominal values of the converters, so we may analyze the peak values during the fault and how the converter is able to provide full power and restrict the power in the maximum allowed limit according to the converter's capacity, such that safe operation is guaranteed. To perform the safe operation of the converter considering the operational limits, a current limitation algorithm is implemented, this algorithm is detailed next.

The GFM control strategy does not rely on the implementation of a current control loop. Due to the nature of the control strategy, i.e., being a voltage source, these control loops then define the basic control blocks to perform GFM, leaving aside the use of the inner current control as done in GFL. Therefore, to limit the maximum current flowing on the converter, the implementation of a current control algorithm might be necessary to perform the current limitation, which can saturate the current to a certain limit during transients. The first straightforward propose is the Current Saturation Algorithm (CSA) carried out in [30]. The CSA strategy is defined as:

$$\begin{cases} |I_{d,sat}| = \min(I_{max}, |I_d|) \\ |I_{q,sat}| = \min(\sqrt{I_{max}^2 - I_{d,sat}^2}, |I_q|) \end{cases} \quad (2.4)$$

where  $I_{d,sat}$  and  $I_{q,sat}$  are the saturated currents of the direct  $I_d$  and quadrature  $I_q$  currents, respectively.  $I_{max}$  is the maximum allowed current in the converter. In order to create a current loop to apply these references, a current loop is created based on the threshold current control principle. This control loop is created by inserting an inverse current control loop using the controlled voltages and the measured current in the converter, therefore, a current control loop is generated to be able to follow a reference. The current loop is only activated during current limitation operation. See the details in [30].

It is required to set a priority for the current component in the CSA algorithm, where active current or reactive current are the possible options. In this case, the direct current component is chosen as priority for the current limitation, which means that the reactive current component will be restricted to the level of active current being supplied and the established limit ( $|I_{q,sat}| = I_{max} - |I_{d,sat}|$ ). The impacts on protection relay performance and operation issues are influenced by the choice of priority given by the current component, but those impacts are not detailed in this study.

In the CSA approach, the system behaves as a current source since the current control is the only one active. Besides the current saturation, when the current limitation is activated the voltage control is not able to really regulate the voltage, therefore, the AC voltage may not keep aligned with the grid voltage, bringing synchronization problems and even instability issues. That is why a second approach for current limitation based on virtual impedance (VI) is also carried out in [30].

The VI approach emulates the effect of an impedance when the current exceeds the maximum allowed value. This strategy is implemented by introducing a voltage drop (from the given virtual impedance) to the voltage references of the voltage control loop, preserving the voltage source feature of the GFM control. Moreover, it can improve the transient stability when compared with CSA method, but nevertheless it can present overshoots during the initial current transients, which is not desirable. Therefore, the parameters tuning of this strategy is very important to properly limit the current and to avoid overshoots when it is activated. The VI strategy is defined as:

$$\begin{aligned} V_d^{ref} &= V_d^* - (R_{VI}I_d - X_{VI}I_q) \\ V_q^{ref} &= V_q^* - (R_{VI}I_d + X_{VI}I_q) \end{aligned} \quad (2.5)$$

with  $V_d^{ref}$  and  $V_q^{ref}$  being the voltage references for the direct  $V_d$  and  $V_q$  quadrature voltages, respectively, considering the virtual resistance  $R_{VI}$  and the virtual reactance  $X_{VI}$ .  $V_d^*$  and  $V_q^*$  are the original references for the voltages before the virtual impedance. The values of the virtual impedance parameters are calculated as follows:

$$X_{VI} = \begin{cases} K_{p,VI} \sigma_{X/R} \Delta I, & \text{when } \Delta I > 0 \\ 0, & \text{when } \Delta I \leq 0 \end{cases} \quad (2.6)$$

$$R_{VI} = \begin{cases} K_{p,VI} \Delta I, & \text{when } \Delta I > 0 \\ 0, & \text{when } \Delta I \leq 0 \end{cases} \quad (2.7)$$

where  $K_{p,VI}$  is the constant gain to calculate to limit the current to a suitable level during the overcurrent in steady state.  $\sigma_{X/R}$  is the virtual impedance ratio used to provide the desired dynamics during the overcurrent to keep a high X/R ratio. The current magnitude is given by  $I_{mag} = \sqrt{I_d^2 + I_q^2}$ , and then  $\Delta I = I_{mag} - I_{max}$  is the current difference between the magnitude and the maximum current that activates the virtual impedance when  $\Delta I > 0$ . The parameters can be calculated according to [31] [32]. This control will be activated only if the magnitude of the measured current overpasses an overcurrent threshold, setting limit the current output of the converter.

In this case, the initial power flow in the AC side is defined and presented in Table 2-7. The power flow in the MTDC is presented in Table 2-8, where the station is absorbing active power from the AC grid (negative values).

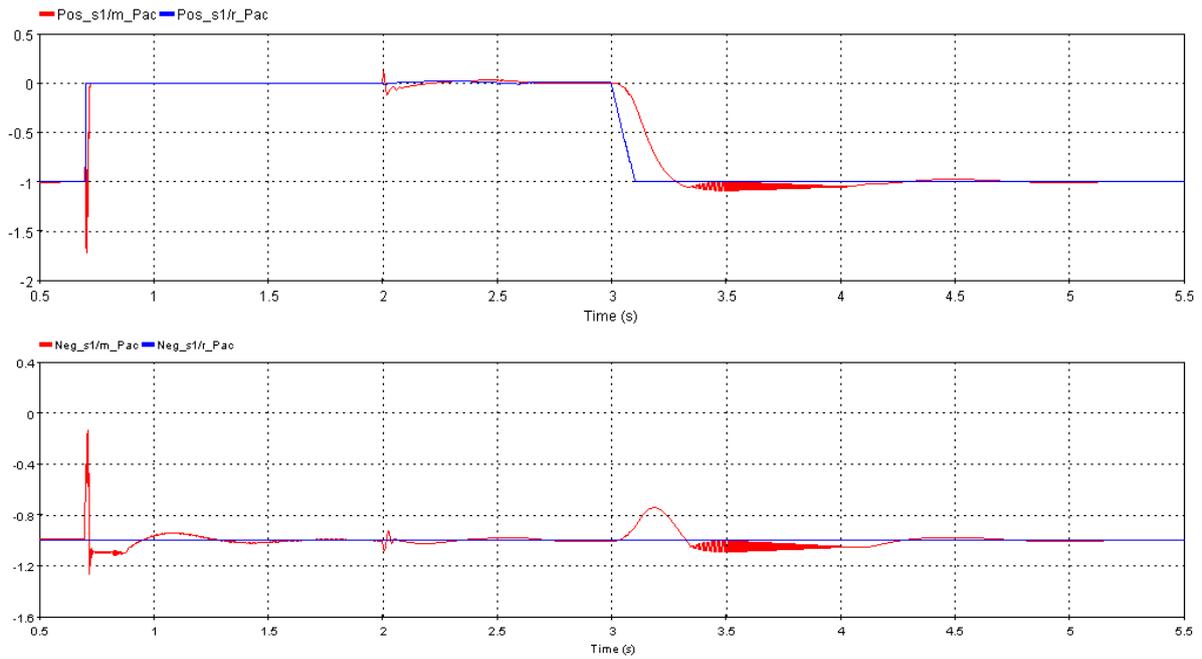
**TABLE 2-7: INITIAL POWER FLOW IN STATION 1 WHEN OPERATING CLOSE TO THE POWER LIMITS.**

STATION	P	Q
Positive Pole – Station 1	-1000 MW	200 MVAR
Negative Pole – Station 1	-1000 MW	200 MVAR

**TABLE 2-8: INITIAL POWER FLOW IN THE MTDC WHEN STATION 1 IS CLOSE TO POWER LIMITS.**

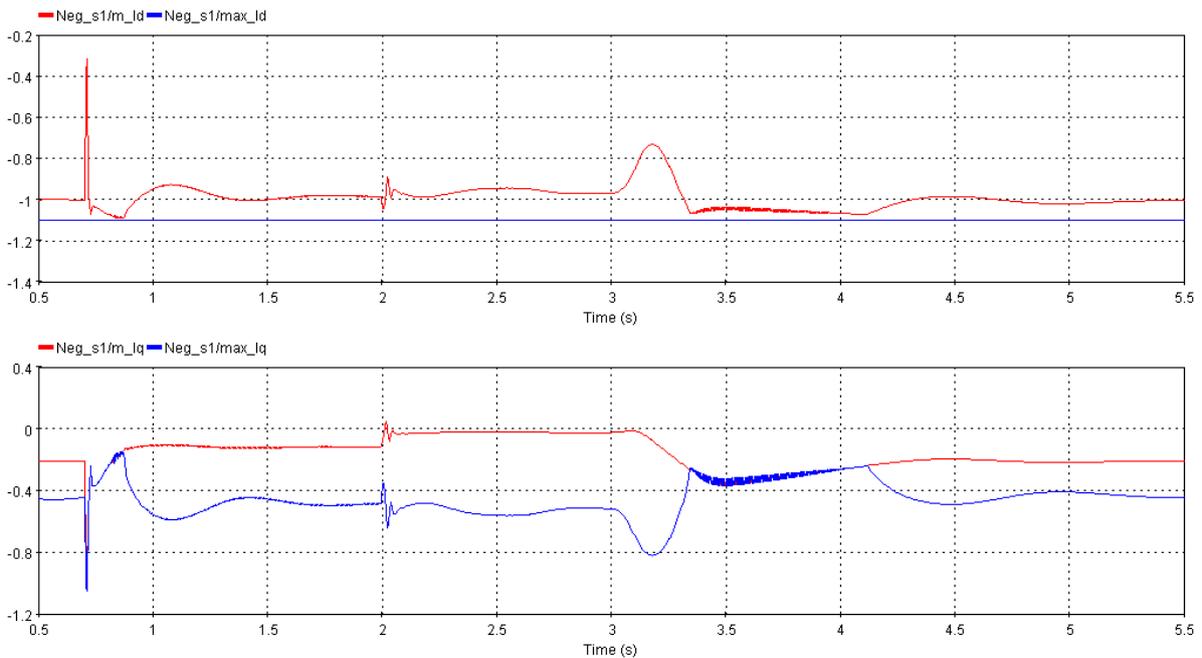
STATION (BIPOLAR)	P	Q
Station 1	-2000 MW	400 MVAR
Station 2	2000 MW	0 MVAR
Station 3	800 MW	400 MVAR
Station 4	-800 MW	400 MVAR

The CSA approach leads to direct limitation of current by the saturation of the current reference at allowed limit when the current limitation is activated. In this case, the maximum current is set  $I_{max} = 1.1$  pu, which is calculated according to the converter’s capacity. Figure 2-37 depicts the power response of the station 1 with the CSA implemented. It is possible to see the current limitation algorithm active right after the fault, to limit the overcurrent of the healthy pole, and also after the active power restoration to limit the current in both negative and positive poles. The currents are properly limited, with a very small overshoot in the first transient, and it is possible to see a high frequency oscillation in power, which is related to the oscillation of the q component of the current limitation. Furthermore, due to the prioritization algorithm, the q component threshold will vary dynamically following the d component behavior. It is when the d component is close to its limits and saturation that the converter has the characteristic output of fast frequency small oscillations.



**FIGURE 2-37: ACTIVE POWER PROFILE IN STATION 1, CONSIDERING CSA APPROACH.**

The CSA approach for current limitation is better seen in Figure 2-38, where the direct current is always kept inside of the limits for the whole simulation, and the activation of the current limitation is evident in the quadrature current, which changes dynamically according to the value of the direct current. So, when the direct current is high, approaching the limits, the quadrature current’s limits is abruptly reduced, activating the current limitation. During this time, preference is given to direct current, which harms the current quadrature, potentially causing synchronism problems. Therefore, a more suitable approach could be used for current limitation, such that the q component is not jeopardized at the expense of the direct current. In this case, the VI approach could be considered a possible solution.

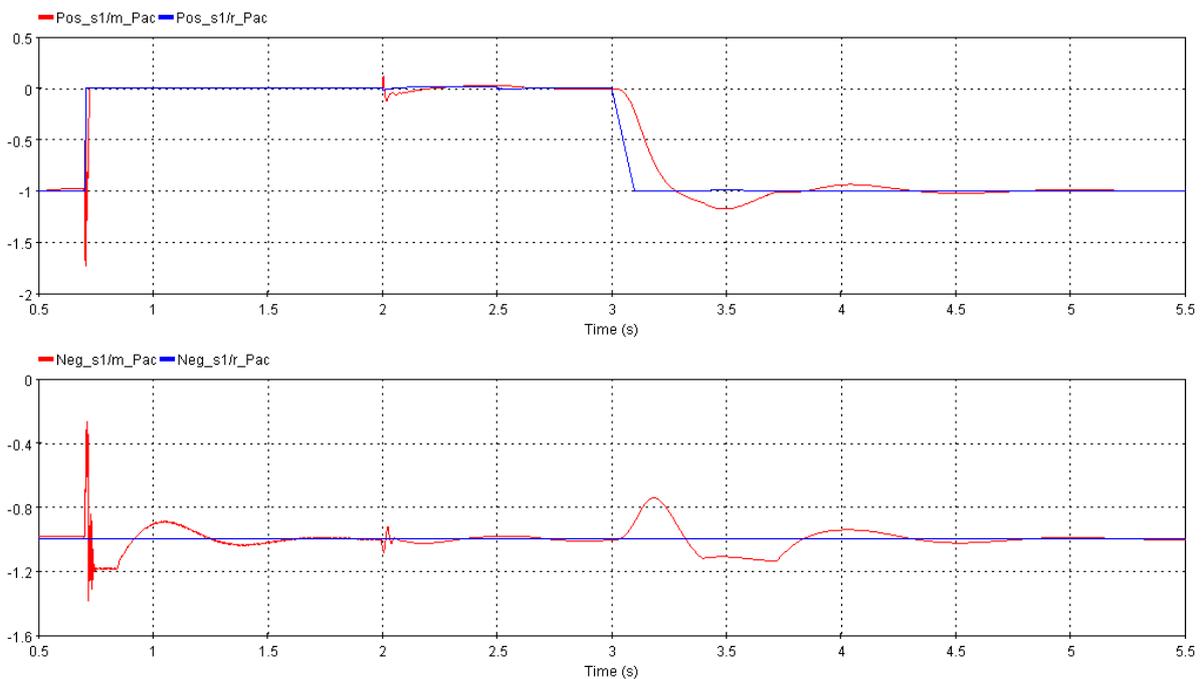


**FIGURE 2-38: ID AND IQ CURRENTS CONSIDERING THE REFERENCE LIMITS FOR CSA APPROACH.**

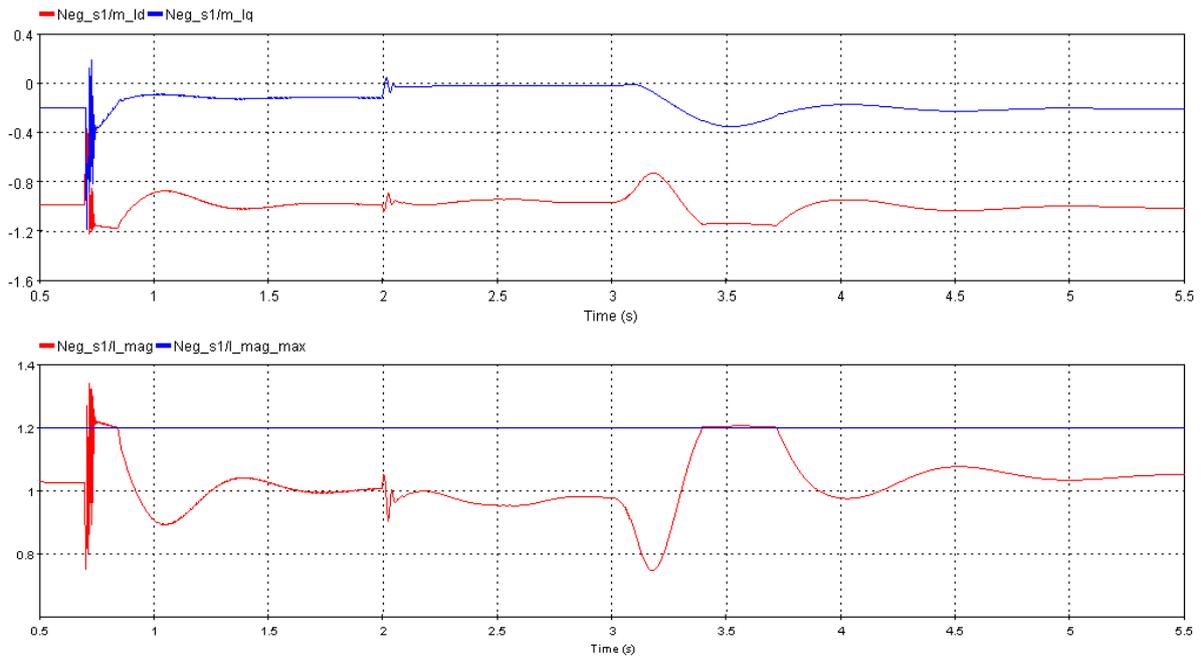
The results of the VI implementation will be presented next. In this case the parameters of the VI approach are given:  $I_{max} = 1.2 pu$ ,  $K_{p,VI} = 0.84$  and  $\sigma_{X/R} = 10$ .

The active power profile in station S1 considering the VI approach is depicted in Figure 2-39, where the action of the current limitation is clearly seen in the healthy pole (Neg\_S1). First, the VI is activated during the DC fault and the healthy converter responds to the fault counteracting the power imbalance by reducing its power supply to the DC grid. Right after, when the converter faces the phase jump, the increase of power supply to the DC side reaches the established limit for current magnitude (1.2 pu), activating the VI strategy. During the first period of VI active, the power and current profile present high frequency oscillations and an overshoot overtaking the established maximum current up to 1.35pu, which is rapidly reduced to the current limits. The oscillations in the beginning of the current limitation can be explained because of the high level of current in both components  $I_d$  and  $I_q$  as shown in Figure 2-40, where there is a conflict to limit both components of the current, since the current limit is given by the current magnitude ( $I_{mag}$ ) also presented in Figure 2-40. The expected behavior of VI approach is to present a current overshoot that is quickly damped until the current limitation is deactivated.

The second activation of VI strategy is after the restoration of active power, where the overshoots of power in the healthy converter is shaved to respect the limit of the current magnitude. Therefore, in this case, the current is properly limited without overshoots, being also under the maximum value. It can be seen that during this period the q component of current is not close to the limit, therefore, only the d component is affected by the current limitation, which makes this operation smoother compared with the previous operation. Figure 2-40 shows that the corresponding current magnitude is limited as the d and q current components are bounded once they reach the current limiting threshold. This leads to the shaved aspect of the power and current signals. Therefore, this approach maintains the VSM characteristic behavior (voltage source) during the current limitation, while maintaining the converter output fenced to the corresponding current threshold.



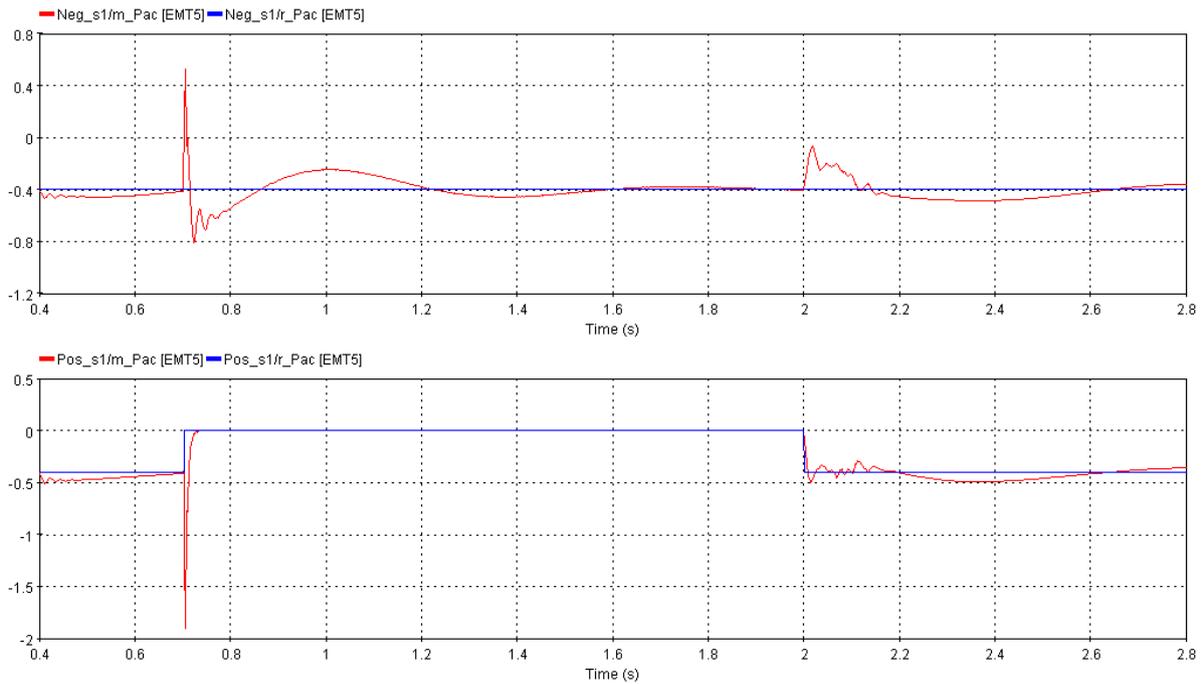
**FIGURE 2-39: ACTIVE POWER PROFILE IN STATION 1 FOR VI APPROACH.**



**FIGURE 2-40: ID AND IQ CURRENTS (TOP), AC CURRENT MAGNITUDE AND MAXIMUM LIMIT (BOTTOM) FOR VI APPROACH.**

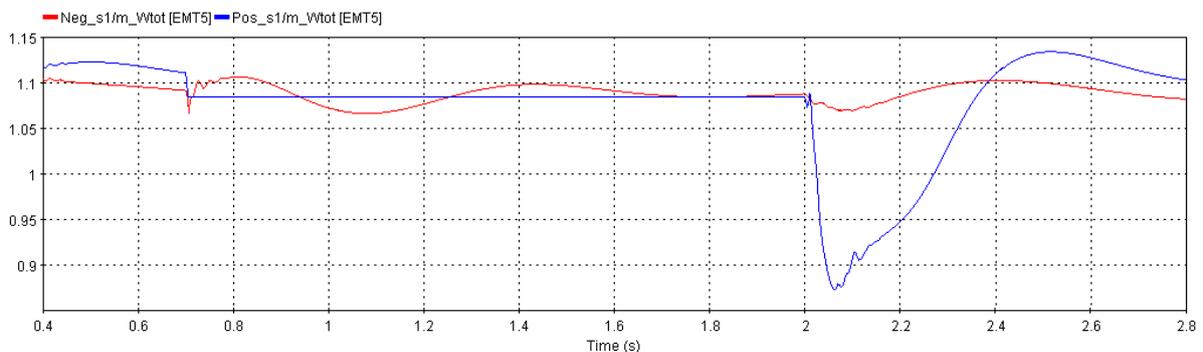
It can be mentioned that an alternative approach to maintain the GFM control during the DC FRT operation without requiring the outer energy control loop proposed here is to maintain the faulty converter blocked until the DCCB is reclosed. In this way, the converter is not able to operate in STATCOM mode, and no voltage support is given by the AC grid during this time. Nevertheless, there is no risk of internal energy imbalance on the faulty converter since no power is requested by the submodules capacitors to control reactive power and AC voltage.

Considering the case where station 1 is operating in GFM mode and there is no possibility to provide reactive power support (by operation restrictions). The faulty converter remains blocked until the DCCB is reclosed (at 2s of simulation). In this case, the power of the faulty pole remains zero until the reclosing of the DCCB and the healthy pole is able to follow its reference after the transient. When the converter is deblocked, the power is also restored at the same time for the faulty converter. Therefore, only the transient of active power restoration is seen, but the reactive power can also be restored at this point. The active power profile of Station 1 is depicted in Figure 2-41.



**FIGURE 2-41: ACTIVE POWER PROFILE IN STATION 1 CONSIDERING THE DEBLOCKING OF THE MMC SIMULTANEOUSLY WITH THE RECLOSE OF THE DCCB.**

The internal energy of the faulty converter is shown in Figure 2-42. It is clear that the internal energy is not disturbed while the converter is blocked, which was kept constant. Therefore, when the DCCB is reclosed, there is a mild transient in the faulty converter due to the restoration of the DC voltage of the converter, and the energy is then controlled to its reference following the GFM dynamics. This figure shows that it is possible to perform this sequence in case the STATCOM operation during the DC FRT is not required.



**FIGURE 2-42: INTERNAL ENERGY OF THE FAULTY POLE WHEN THE DEBLOCKING OF THE MMC OCCURS SIMULTANEOUSLY WITH THE RECLOSE OF THE DCCB.**

## 2.3. Including Frequency Dynamics in the AC Grid

In this section, the inclusion of frequency dynamics in the AC grid is considered through the integration of a synchronous machine to model the AC grid, which comprises more complex dynamics to perform the analysis of the DC FRT. This approach approximates the frequency dynamics of a conventional grid where synchronous generators are the dominant source of power and inertia. Therefore, it is possible

to differ the conventional grid from the power electronic based grid that is going to be detailed in the next section. The DC fault can also impact frequency and angle dynamics in the AC grid mainly considering the GFM control of the converters station connected to the AC grid, therefore it is important to analyse the impacts of a DC FRT system operation into the grid frequency and how its behaviour is affected by the frequency dynamics.

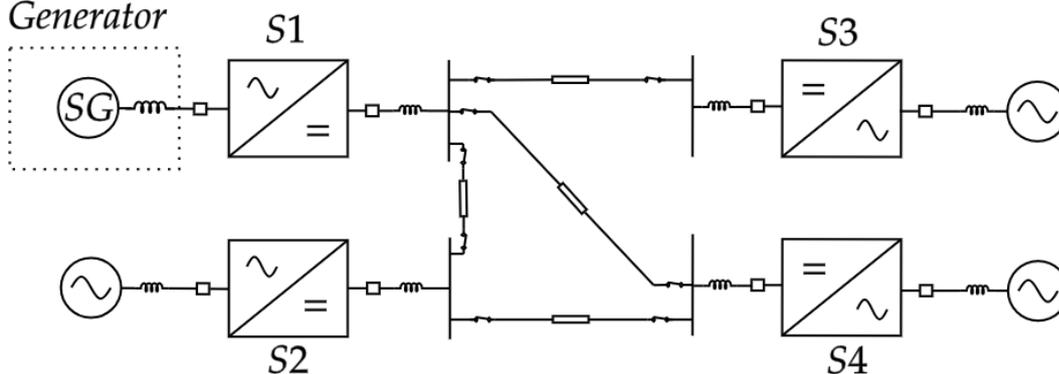
The AC grid is now modelled by a synchronous generator of 10 GVA of nominal power and 400kV of nominal voltage, with an inertia coefficient of  $H_{SG} = 2s$ , with a frequency droop control (4% coefficient) and the turbine dynamics are modelled as a lead-lag filter ( $F_{SG} = s + 1/s + 6$ ). The parameters of the machine are presented in Table 2-9.

**TABLE 2-9: ELECTRICAL PARAMETER OF THE SYNCHRONOUS MACHINE.**

PARAMETER	VALUE (PU)	PARAMETER	VALUE (PU)
$R_a$	0.002	$R_f$	0.0067
$X_0$	0.188	$X_f$	1.4426
$X_d$	1.394	$X_{af}$	0.9847
$X_l$	0.188		
$X_q$	1.353		

The SCR of the grid is kept in SCR=1.9 according to the equivalent impedance of the grid, where only the impedance of the AC lines impedance is considered in the SCR calculation (electrical distance). As in the previous case, the four stations are in bipolar configuration, station 1 is operating in P-mode control, while the rest are performing Vdc control with the same droop coefficient, consequently the three remaining stations share in the same proportion the DC voltage control. The power flow is according to Table 2-3. The C&P coordination sequence is the one presented in Figure 2-3, resulting in a temporary stop of 400 ms. In this case, it is not necessary to extend the sequence as done before, since the characterization of the GFM converter has been already presented, and now the focus is on the interactions between the control and the protection strategies.

*Synchronous Generator*

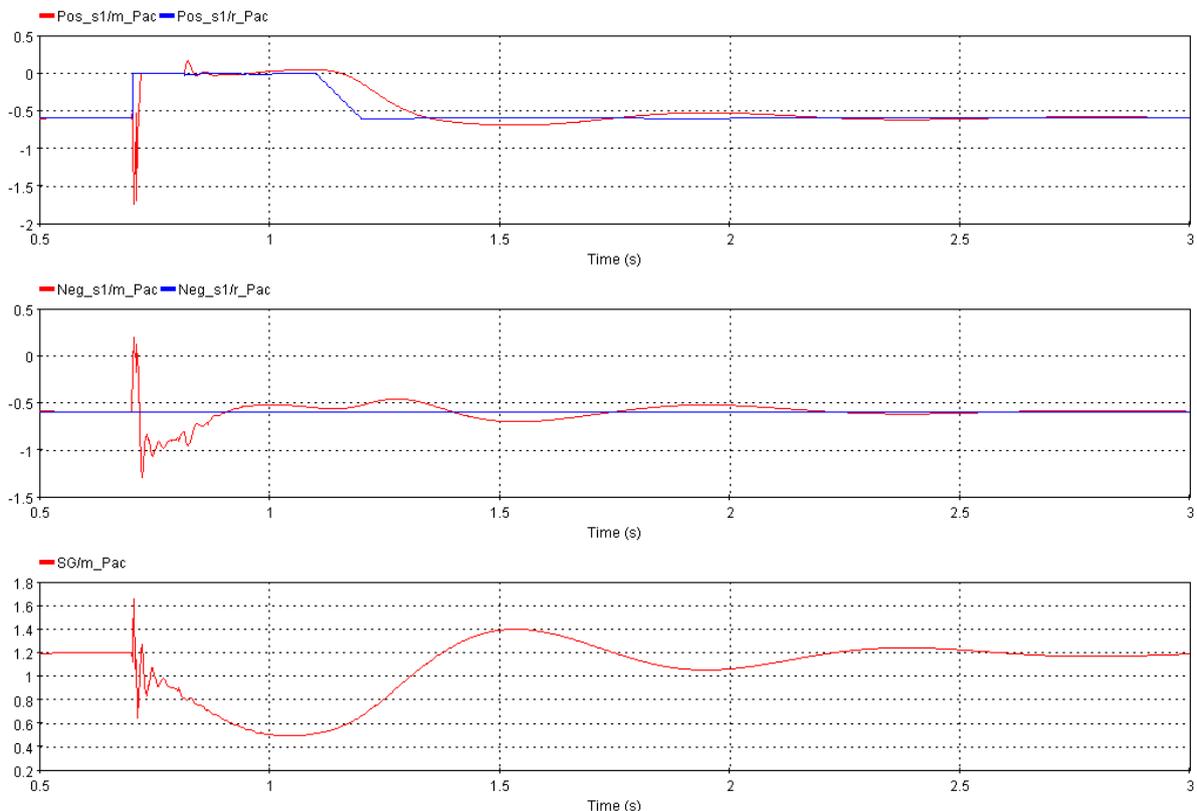


**FIGURE 2-43: ELECTRICAL MODEL OF SYNCHRONOUS MACHINE CONNECTED TO THE MTDC MESHED GRID.**

It is expected that the frequency dynamics can impact the DC FRT operation when the converters are GFM control mode. The GFM control implemented with VSM has an inertial response, which means that frequency variations (RoCoF) could cause a power reaction from the GFM control. Therefore, since the frequency of the synchronous machine is still varying during the DC FRT, the frequency

support from the VSM could cause a power reaction affecting the converter's operation during the DC FRT.

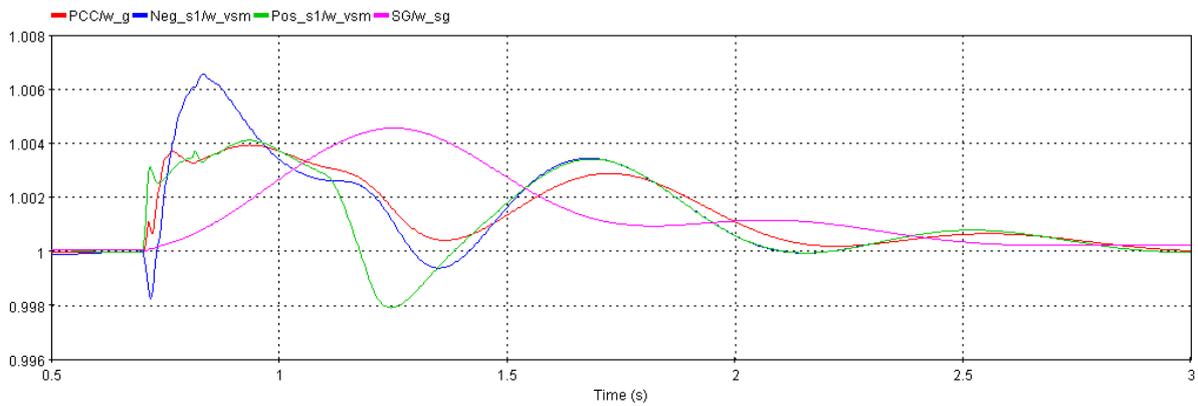
The active power profile of the station 1 and from the synchronous machine connected to the AC side of the grid are shown in Figure 2-44. The initial power transient of the fault is quite close to the other simulations when considering GFM control for both healthy and faulty poles. Here, the temporary stop is reduced to 400 ms, even so, power fluctuations are not considerable during the DC FRT process, where a small peak can be seen when the faulty converter is deblocked. When the active power is restored in the faulty converter, there is reasonable transient in power, which is also reflected in the healthy pole. At this point, it is noticed that the dynamics of the systems are now slower, and the power transients lasts longer, which is highlighted by the power measured in the synchronous machine, presenting a settling time longer than 2 s.



**FIGURE 2-44: ACTIVE POWER PROFILE IN STATION 1 CONNECTED WITH A SYNCHRONOUS MACHINE.**

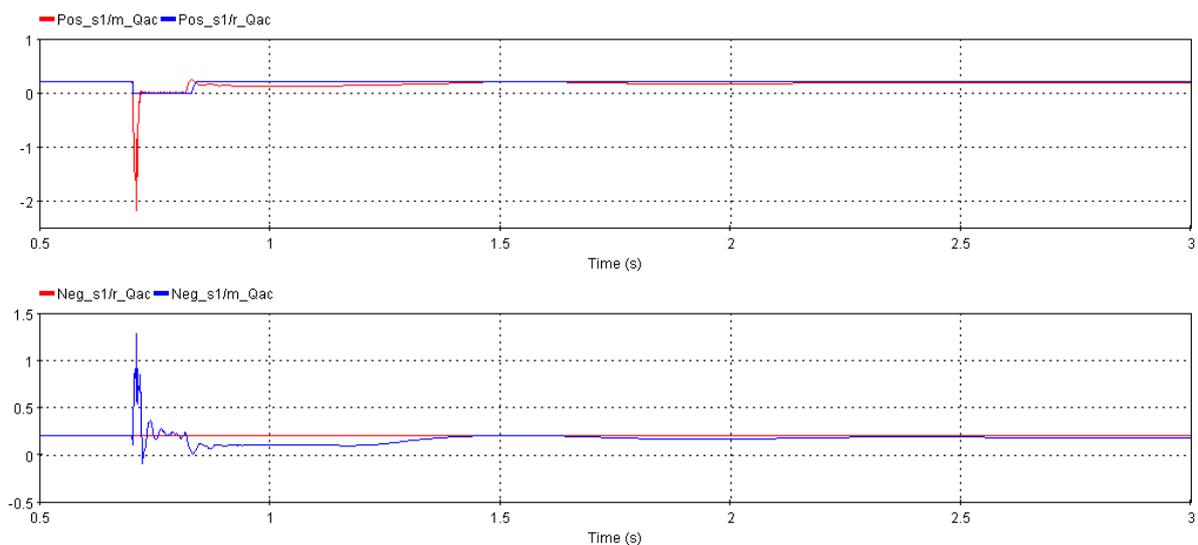
The frequency dynamics of the system are presented in Figure 2-45, where the computed VSM frequency of positive and negative poles, the synchronous machine frequency and the PLL frequency ( $\omega_g$ ) are shown. Initially, the faulty pole frequency (in green) has a fast growth, since there is a sudden request for power to the DC side of the grid because of the DC fault. On the other hand, the healthy converter has a sudden drop in frequency (in blue) reacting to the power imbalance on the AC grid, reducing the power supply to the DC side, such that power support is provided to the AC grid. After this first transient, the healthy converter reacts to the disconnection of the positive pole of the DC grid (DCCB is opened), which is seen as a phase jump, so it increases its power supply to the DC grid in response to that. As a consequence, the frequency of the healthy converter also increases, then going to a new equilibrium point. The frequency of the synchronous machine (in pink) reacts to the power shift in the grid (the power stop of the faulty converter), which is seen as a load disconnection.

Therefore, the SG frequency increases to reach a new equilibrium point, but at 1.1 s of simulation, the active power is restored in the faulty converter, bringing the frequency down to the original equilibrium point following its dynamics. The VSM converters also react to the active power restoration, therefore the frequency is reduced as a reaction of the new operating point. In this case, the reaction of the frequency in the faulty converter is stronger since it is the one where the power reference has been changed.

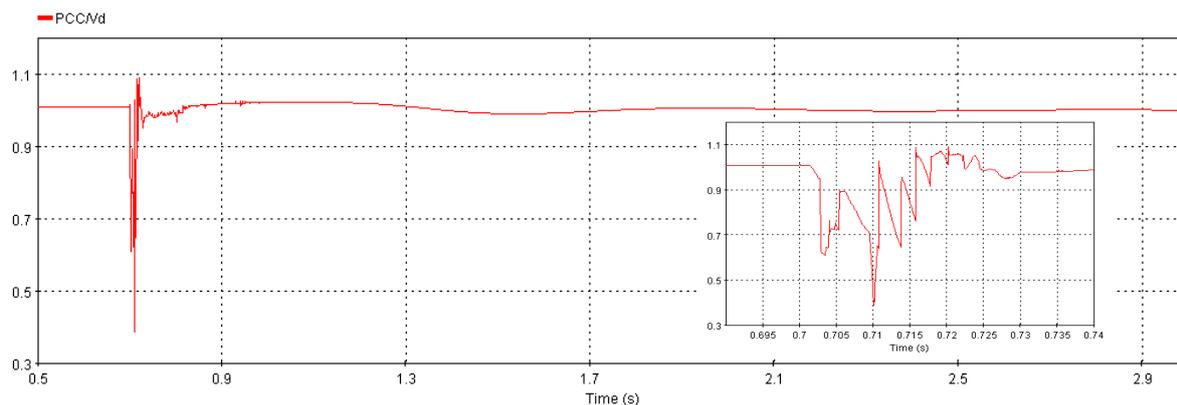


**FIGURE 2-45: FREQUENCY DYNAMICS OF THE SYSTEM CONSIDERING STATION 1, SYNCHRONOUS MACHINE AND THE PLL MEASUREMENT.**

The reactive power profile of the Station 1 is depicted in Figure 2-46, which is quite similar to previous simulations with an initial strong overshoot then going to the new operating point, but in this case the deblocking of the MMC and the reactive power restoration happens approximately 100ms after the fault, quickly starting the STATCOM mode. Therefore, the AC voltage is quickly restored to the original levels, being much less deteriorated, this can be seen as an advantage for the rapid action of the coordination sequence. The AC voltage profile present a higher drop during the fault when the synchronous machines in considered (which is handle by a AVR control) but has a smoother behavior considering the whole DC FRT as is shown in Figure 2-47.



**FIGURE 2-46: REACTIVE POWER PROFILE IN STATION 1 CONNECTED TO A SYNCHRONOUS MACHINE.**



**FIGURE 2-47: THE AC VOLTAGE MAGNITUDE AT THE PCC WHEN THE SYNCHRONOUS MACHINE IS CONNECTED.**

### 2.3.1. Oversizing the converters

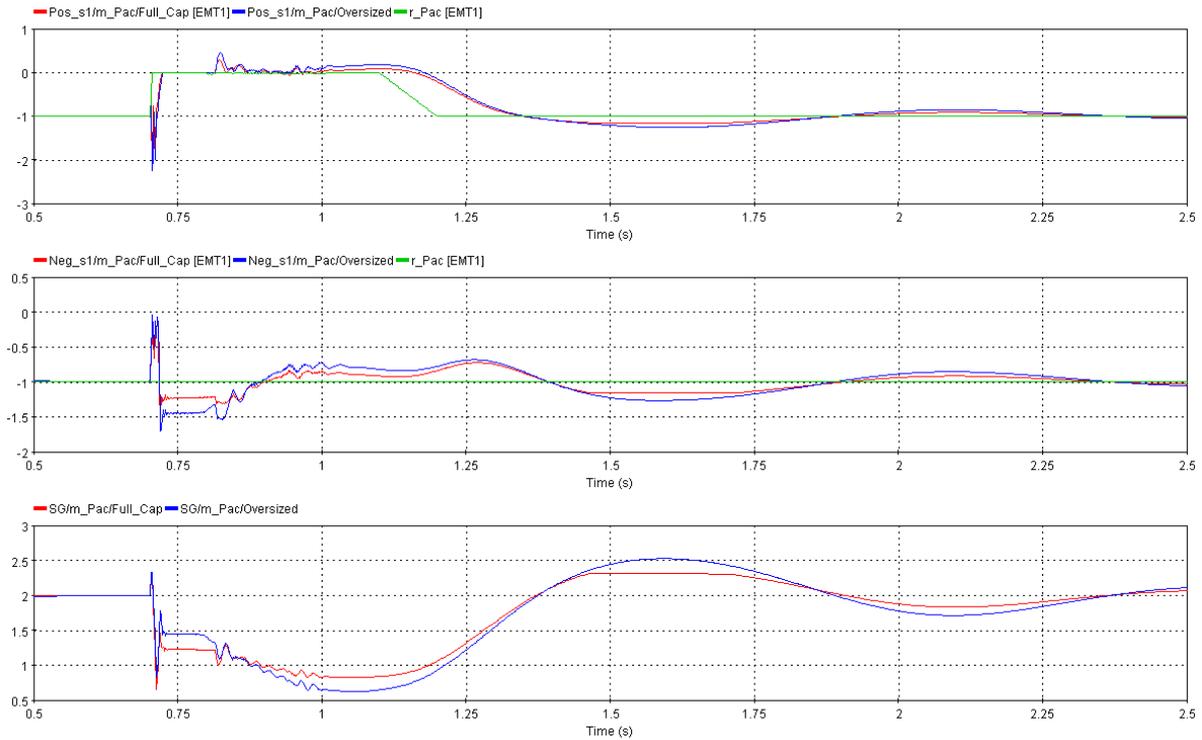
This subsection proposes a strategy for oversizing converters that provide ancillary services to the AC grid. The concept involves maintaining the existing grid configuration while increasing the nominal power capacity of the converters by 20%. This additional capacity creates extra headroom that can be utilized for providing services to support the AC grid.

Importantly, this approach does not require adjustments to the sizing of surrounding equipment and cables, allowing the overall system to retain its original size. The additional power capacity is intended for transient use only. Consequently, the system can continue to provide support to the AC grid even when the converter is fully dispatched, providing an additional operational margin for voltage and frequency support. This advantage is particularly notable when employing GFM control of the converters, especially in VSM strategy.

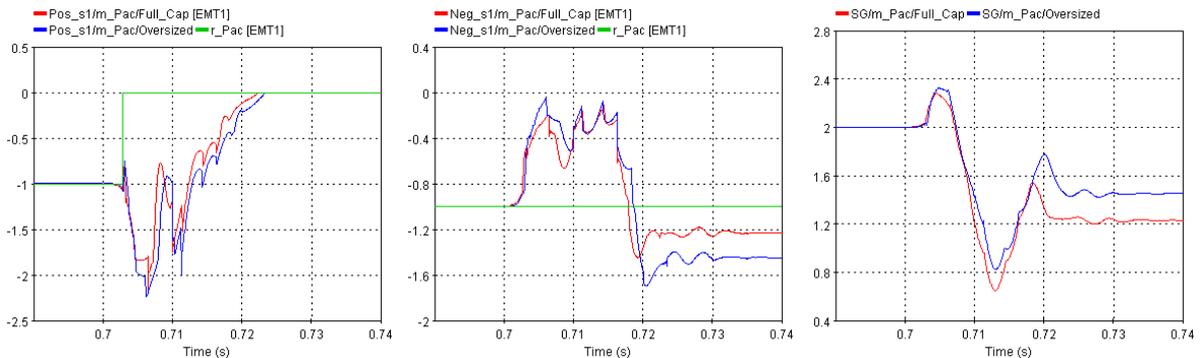
However, analyzing this strategy requires the system to operate close to its limits. Therefore, the system operates based on the power flow specified in Table 2-7 and Table 2-8.

It's important to note that current limitation operation is activated when the converter operates near its operational thresholds to ensure that the current remains within predefined limits. However, in the event of a DC fault, if the converter has been oversized with 20% extra capacity, this surplus power can be utilized to meet the increased demand during transient periods caused by the fault. This can be seen in the power profiles of Station 1 presented in Figure 2-48. In this case, the base power remains the same ( $S_{base} = 1000MVA$ ), so the oversized converter will present the same value in per unit concerning to the power references and steady state, but it is going to be able to go further on power supply during the transients. It can be seen that the faulty pole has a similar behavior when comparing the normal size with the oversized converter, but the oversized converter presents a slightly higher current peak during the fault as it is shown in Figure 2-49. The great advantage is in the healthy pole, where the oversized converter is able to provide more power support during the first moment of the fault to reduce the power imbalance, but also during the phase jump seen by the healthy converter providing close to 1.5 pu power to the DC grid (shaved by the current limitation operation). In this case, the current limitation is also activated in the normal size converter (healthy pole) during the transient after the active power is restored, while in the oversized converter, the current limitation is not triggered because of the extra available power.

### D3.3: Protection Concepts



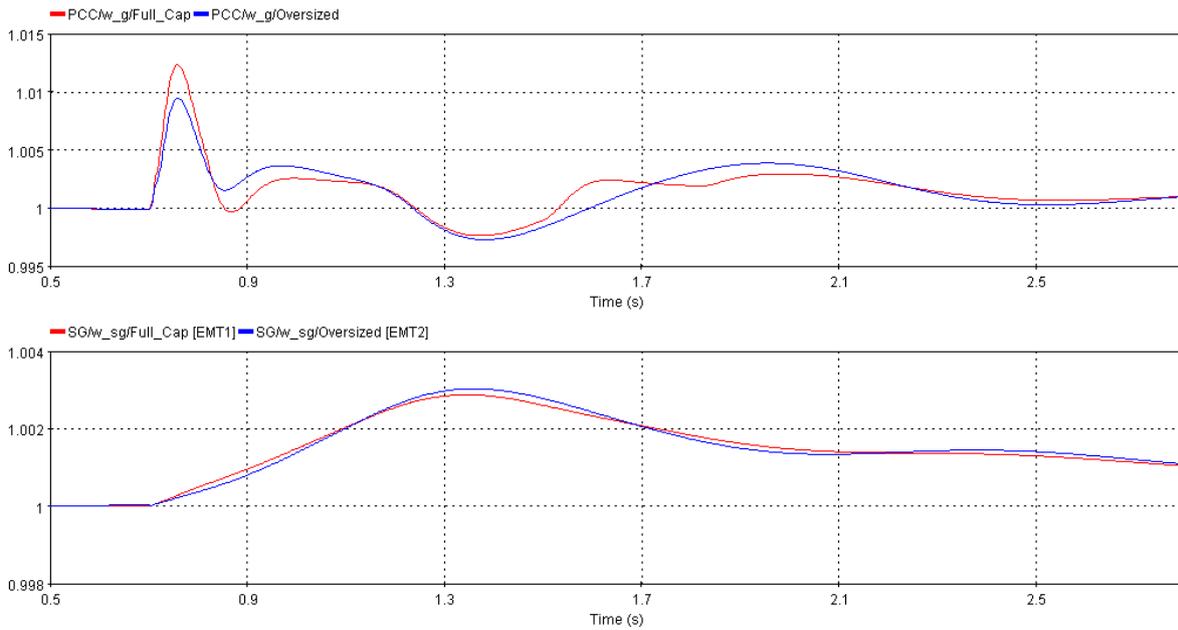
**FIGURE 2-48: ACTIVE POWER PROFILE IN STATION 1 CONNECTED WITH A SYNCHRONOUS MACHINE.**



**FIGURE 2-49: ZOOM IN THE ACTIVE POWER PROFILE IN STATION 1 CONNECTED WITH A SYNCHRONOUS MACHINE.**

The impact of the oversized converter also appears in the frequency of the grid, the PLL frequency and the frequency of the synchronous machine is depicted in Figure 2-50. It can be seen that the frequency calculated by the PLL in the oversized converter case has an improved nadir and RoCoF. This is because the oversized converter is able to provide more power during DC FRT, reducing the consequent effect in frequency. Therefore, the VSM frequency for the converters is more impacted by oversized the converter. Nevertheless, the frequency of the synchronous machine is slightly reduced in RoCoF during the first transient, but it results in a slightly higher nadir.

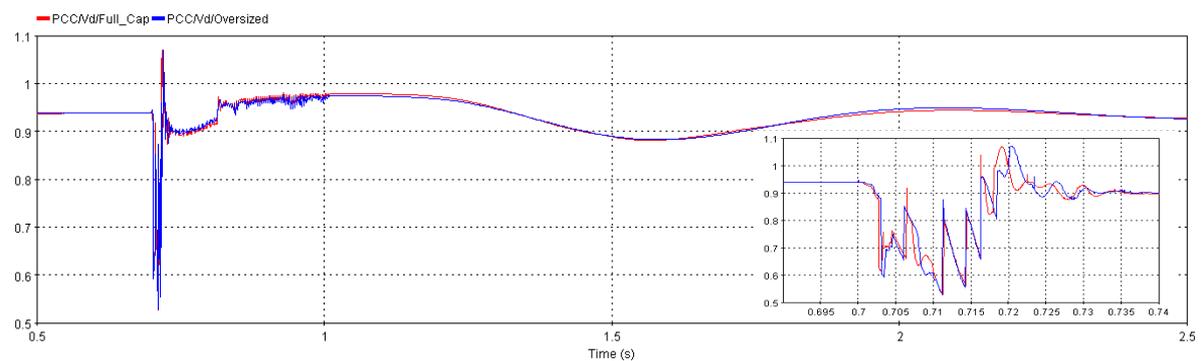
### D3.3: Protection Concepts



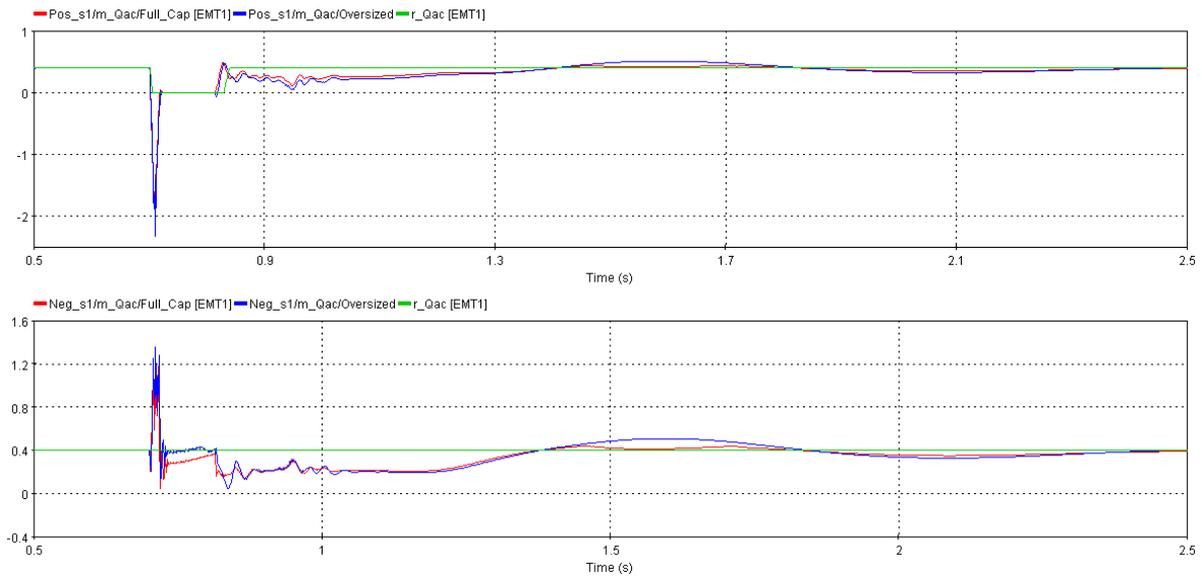
**FIGURE 2-50: FREQUENCY DYNAMICS OF THE SYSTEM CONSIDERING STATION 1, SYNCHRONOUS MACHINE AND THE PLL MEASUREMENT.**

On the other hand, the AC voltage is not directly affected by the converter being oversized as can be seen in Figure 2-51. The AC voltage profile is quite similar when comparing the oversized converter with the original one. The reactive power presents a slight advantage with the oversized converter. During the time in between the converter deblocking and the reclose of the DCCB, the oversized converter has more room to provide reactive power, maintain the reactive power level at the desired reference, while the original size converter is more limited to provide the support to reactive power.

Indeed, oversizing converters can offer benefits when handling power transients near their operational limits. This extra capacity enables converters to manage sudden power fluctuations effectively. However, the decision to invest in such oversizing depends on the significance of this ancillary service for the AC network and the associated costs of this investment. System operators have considered this possibility, suggesting it warrants further exploration beyond DC FRT operations.



**FIGURE 2-51: THE AC VOLTAGE MAGNITUDE AT THE PCC WHEN THE SYNCHRONOUS MACHINE IS CONNECTED.**

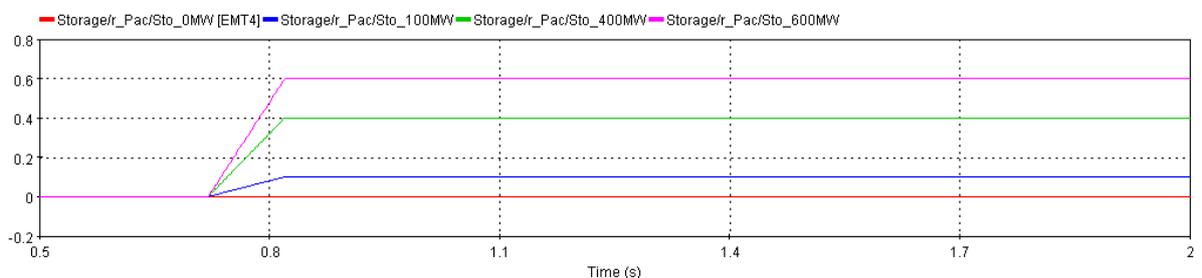


**FIGURE 2-52: REACTIVE POWER PROFILE IN STATION 1 CONNECTED TO A SYNCHRONOUS MACHINE.**

### 2.3.2. Energy Storage Insertion

In this section, we introduce an energy storage system (ESS) connected to the AC side of the grid, forming a new converter component. The power converter interfaces the energy storage and the AC grid being connected at the PCC. The ESS controls power output (P and Q) based on a specified reference. As a frequency containment reserve (FCR), the ESS objective is to help maintain power balance on the AC side during disturbances in the DC system, thereby mitigating impacts on the AC grid using stored energy. The energy storage system can employ either GFM control, reacting naturally to power fluctuations, or GFL control, activated solely to provide power as needed.

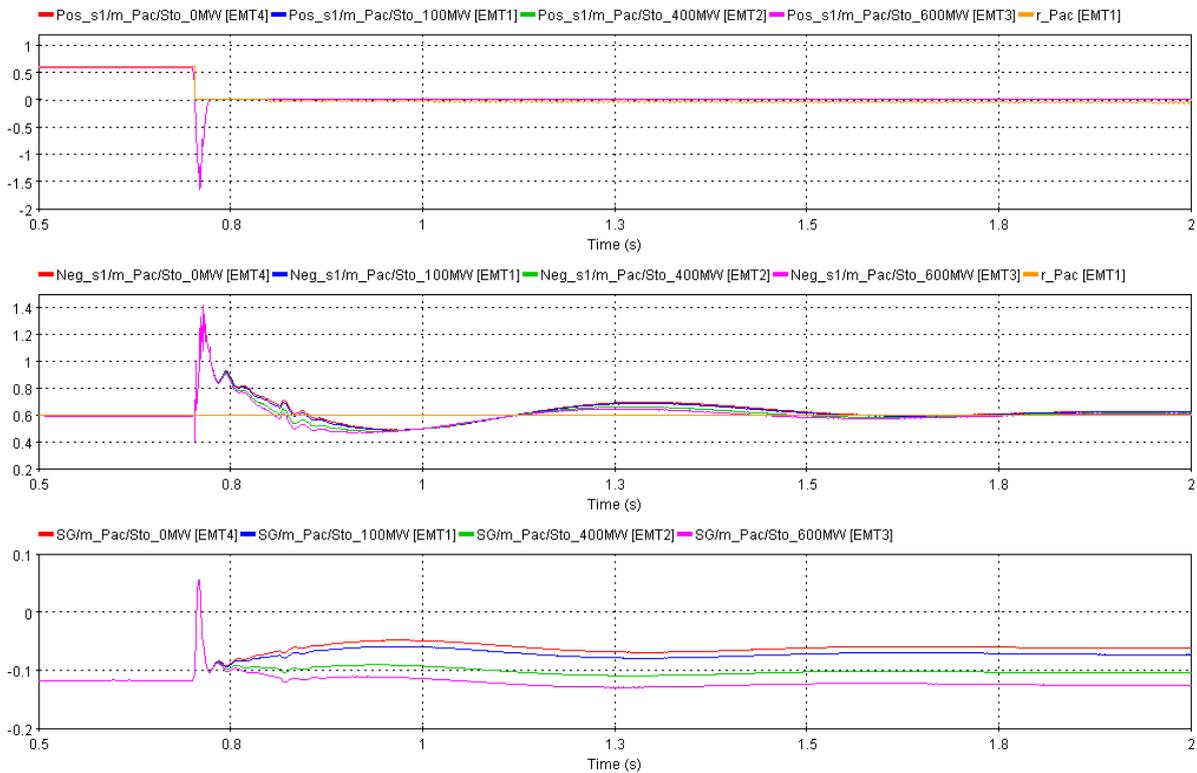
In the first scenario, the energy storage operates in GFL mode. Furthermore, since converter station 1 is injecting power into the AC grid, the temporary stop of the faulted pole converter is seen as a generation loss. Therefore, the ESS contributes to the AC grid stability by injecting power the mismatch power. Power dispatch from the storage begins when the DC breakers open, considering a 10 ms communication delay, with a ramp-up of 100 ms to reach the given reference. Four scenarios are examined, varying the power injected by the ESS: 0 MW, 100 MW, 400 MW, and 600 MW. Figure 2-53 illustrates the power reference for the ESS under each scenario.



**FIGURE 2-53: ENERGY STORAGE ACTIVE POWER REFERENCE PROFILE.**

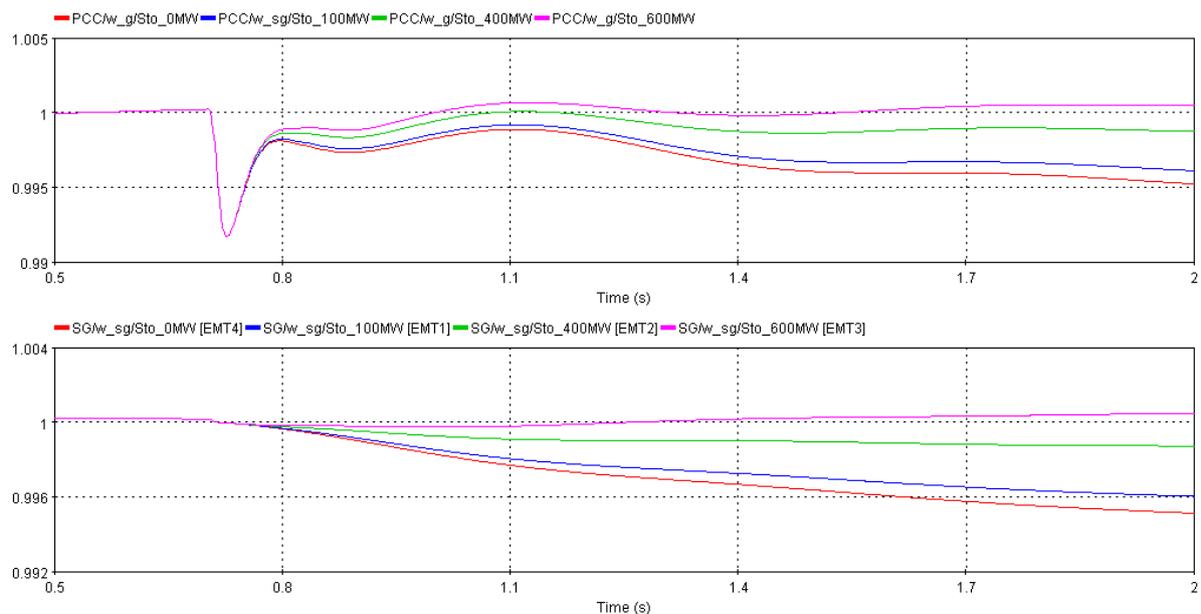
The power profile on the converter station and on the synchronous machine considering the different power level supplies of the ESS are depicted in Figure 2-54. The initial response to the fault is like as presented in previous cases since the action of the ESS starts after 20ms of the fault. Therefore, the

peaks of power are not changed because of the ESS. Once the ESS is supplying power, it is possible to see the relief of power from the synchronous machine and the healthy converter, where the ESS is contributing to the power balance of the system. As expected, the higher level of storage the higher reduction of power injected by the healthy converter and by the synchronous machine.



**FIGURE 2-54: ACTIVE POWER PROFILE IN STATION 1 CONNECTED WITH A SYNCHRONOUS MACHINE.**

The frequency of the synchronous machine and the PLL frequency at the PCC are depicted in Figure 2-55. Here, it is clearly seen that the ESS really provides frequency support to the AC grid by injecting power into the PCC. The frequency of the synchronous machine is less disturbed according to the level of power injection by the ESS, where its nadir is also reduced according to the level of power in the ESS. When the ESS is supplying 600 MW, which is exactly the same level of power imbalance, the disturbance on the SG frequency is minimum, where the frequency is completely restore in steady state, i.e., the final frequency level is the same as the initial value. Considering the PLL frequency on the PCC, it is possible to see the frequency dynamics of the VSM converters considering insertion of the ESS. As expected, the initial transient is not supported by the ESS, but the frequency support is seen for the steady state level of frequency for each power level supply scenario. This can be considered as a good AC grid support, which can be considered as a solution using FFR strategy.



**FIGURE 2-55: FREQUENCY DYNAMICS OF THE PLL MEASUREMENT AT THE PCC AND THE SYNCHRONOUS MACHINE.**

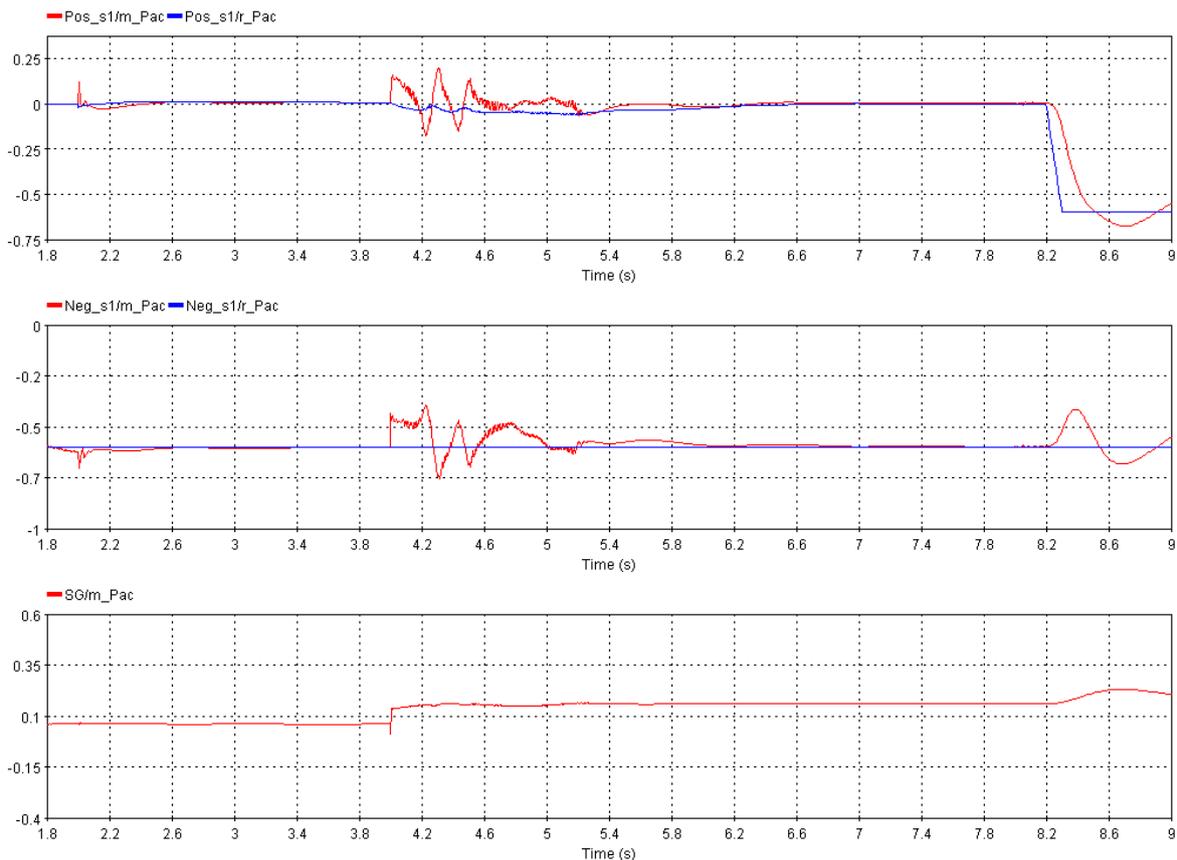
### 2.3.3. Frequency dynamics interaction (VSM and SG)

In this section, the possible frequency dynamics interaction between the VSM converters and the synchronous machine is investigated. The GFM control strategy is designed to share the responsibility of maintaining the AC grid frequency and voltage. Therefore, the VSM converters naturally react to frequency variations in the grid by providing/absorbing power to contribute to frequency stability. By including the frequency dynamics of the grid in the analysis, we can see the interactions between the VSM converter and the grid frequency when the frequency is disturbed, e.g. a frequency RoCoF variation from a load shift or a generation loss. So, the purpose is to analyse the possible interferences of frequency dynamics during the DC FRT operation in the converter stations when GFM control is implemented.

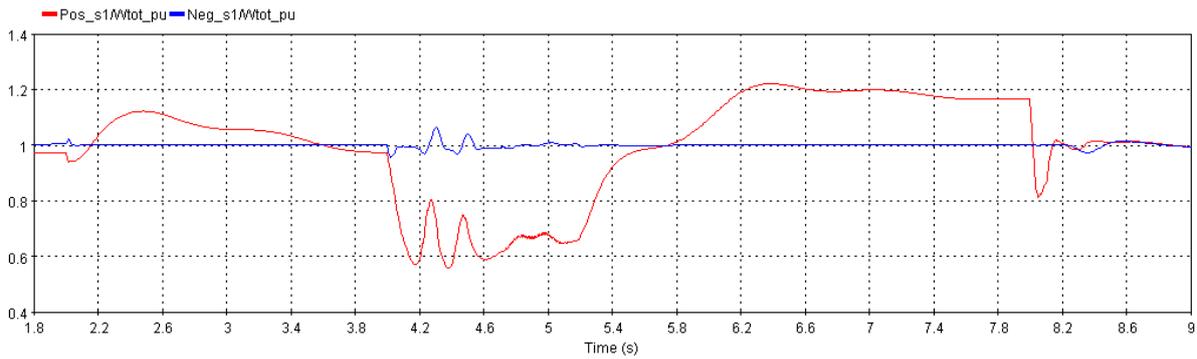
The influence of the frequency dynamics is investigated here by inserting a frequency disturbance during the DC FRT operation. In this case, the disturbance can be interpreted as a load connection, which creates a frequency RoCoF after the faulty converter is deblocked, but before the DCCB is closed. Then, the DC side of the grid is not available to support the AC grid, but because of the VSM feature to react to frequency variations, the faulty pole in GFM will change its active power reference to support the AC grid. Of course, the healthy pole also is going to respond to that disturbance causing a general transient in the system.

In this case, the C&P sequence is extended to better analyze the dynamics of the FRT. The initial sequence remains the same as before: the DC fault happens at 0.7s; the faulty pole is blocked about 2.5ms after the fault and the DCCB is opened at 0.710s of simulation; once the fault is cleared, the faulty pole is deblocked at 2s. During this period, at 4s of simulation, a load shift of 1000MW is connected beside the synchronous generator to create the frequency perturbation required to analyze the VSM control. Finally, the DCCB is reclosing is extended to reclose at 8s of simulation, allowing the transient analysis of the power perturbation. DC voltage and reactive power is restored at 8.1 and active power is restored at 8.2s.

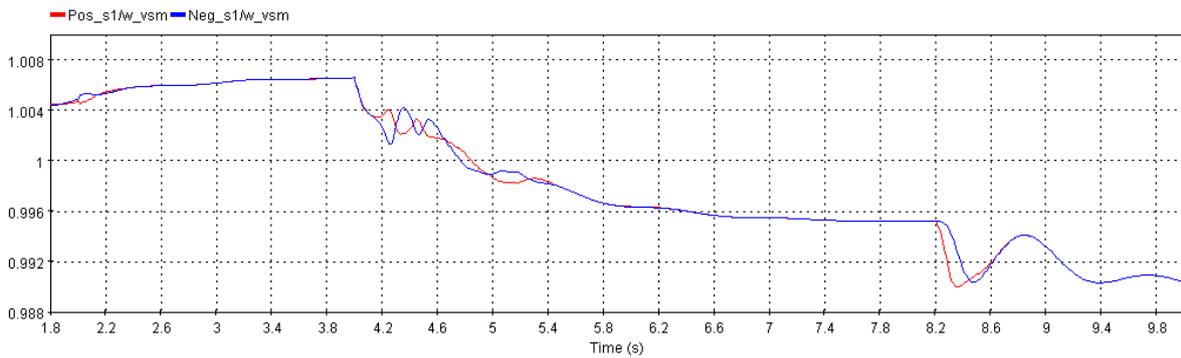
Figure 2-56 depicts active power response of station 1 in GFM control. At the moment of the load shift, both healthy and faulty converters react to support the AC grid compensating for the power imbalance. The healthy converter reduces the power flow to the DC grid and the faulty converter injects power to the AC grid, they are exchanging power creating a low frequency oscillation, which can be clearly seen in the computed VSM frequencies of the converters, depicted in Figure 2-60. This is seen as a natural response to frequency perturbation, but the faulty pole is not connected to the DC grid yet, therefore, the internal energy of this converter is highly affected. The internal energy is depicted in Figure 2-57, showing that the internal energy is drastically reduced to supply the required power to the AC grid, therefore the external energy control loop takes action to balance the internal energy. Therefore, the action from the VSM to compensate the power in the AC grid and the action of the outer control loop for internal energy conflicts in between supplying and absorbing power from the AC side of the grid, highlighting the power oscillations during this transient. Next, after 5.4s of simulations the frequency oscillations are damped, so there is no power exchange between the converters and the frequency of the synchronous machines reaches a new equilibrium point. During this period, the faulty converter is not required to support the AC grid, allowing the energy to be slowly controlled back to its reference. The load shift perturbation has a high influence on the GFM converters, and it brings power oscillations to station S1, if the DC FRT operation is in between the deblocking and the reclosing of the DCCB, since outer loop of energy control needs also to play a role in this case.



**FIGURE 2-56: ACTIVE POWER PROFILE IN STATION 1 CONNECTED WITH A SYNCHRONOUS MACHINE, WHEN CONSIDERING THE LOAD SHIFT.**

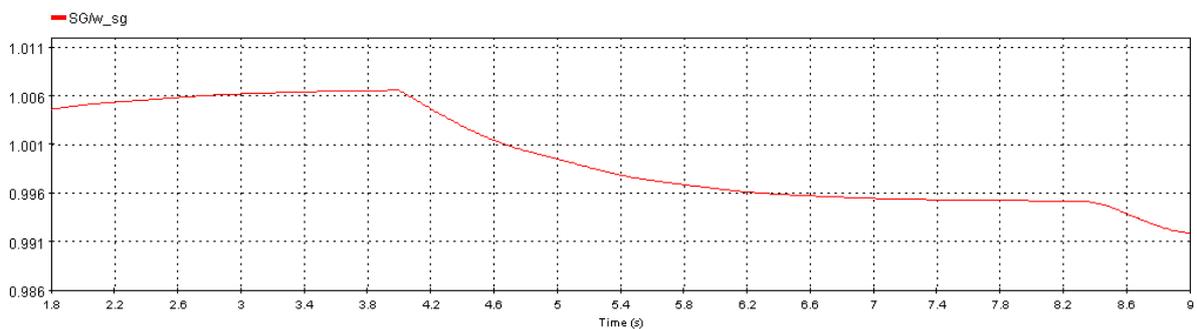


**FIGURE 2-57: INTERNAL ENERGY OF THE POSITIVE AND NEGATIVE CONVERTERS FROM STATION S1.**



**FIGURE 2-58: VSM FREQUENCY OF THE CONVERTERS IN STATION S1.**

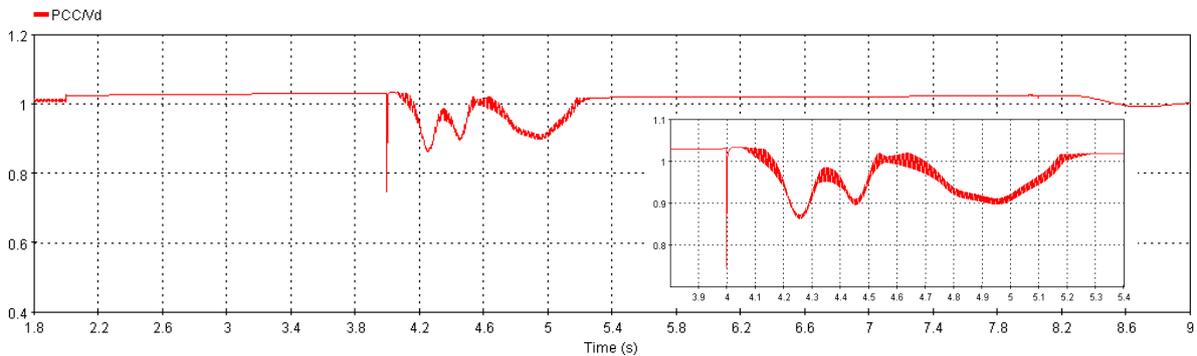
The frequency of the synchronous generator is depicted in Figure 2-59, where the dynamics of the frequency caused by the load shift is highlighted. This load shift perturbation induces an initial RoCoF of 0.5Hz/s and reaches a new equilibrium point close to 49.75Hz. It can be seen the after 5.4s the frequency variations have been already reduced, so the response of the VSM converters is going to be also reduced. As expected, the frequency of the synchronous machine is affected by the oscillations of the VSM frequencies, since the machine is much bigger than the converters of station S1, and it is considered a weak grid scenario ( $SCR=1.9$ ), i. e. a high electrical distance between the synchronous machine and station S1.



**FIGURE 2-59: FREQUENCY DYNAMICS OF THE SYNCHRONOUS MACHINE.**

The AC voltage on the PCC is depicted in Figure 2-60, which is highly affected by the transient of the load shift. When VSM converters share voltage control at the Point of Common Coupling (PCC), any power disturbance tends to have a greater impact on AC voltage. This occurs because the faulty pole fails to supply reactive power adequately, as its action to provide power support to the AC grid

conflicts with the outer energy control loop. Consequently, the internal energy balance is compromised, preventing proper voltage control by supplying the necessary reactive power. Furthermore, the healthy converter is also affected by the disturbance, leading to limitations in AC voltage control for both converters. These limitations result in the variations observed in Figure 2-60.



**FIGURE 2-60: THE AC VOLTAGE MAGNITUDE AT THE PCC CONNECTED THE SYNCHRONOUS MACHINE, WHEN CONSIDERING THE LOAD SHIFT.**

### 2.3.4 Local RoCoF Index

The Rate of Change of Frequency (RoCoF) serves as a crucial metric for assessing AC system stability, offering insights into the magnitude of perturbations within the AC grid. Compliance with defined RoCoF limits is pivotal from a protection point of view, triggering protection actions such as disconnecting generators or initiating load shedding when these limits are exceeded. Thus, an examination of frequency dynamics within the AC/DC system is directly related to RoCoF values analysis. The idea of this section is to bring the concept of local RoCoF, such that this variable can be used as an index to evaluate the systems performance referring to reliability and resilience parameters.

The term "local RoCoF" refers to RoCoF measurement at generator terminals, providing a localized assessment of frequency dynamics essential for identifying the effects of temporary converter loss on neighboring synchronous generators (SGs). It means that local measurement of RoCoF can differ from the centralized measurement units, triggering locally protection actions and breakers. This can affect the system operation, since from the global point of view, the RoCoF measurements can be inside of the requirements, but locally they can exceed the established limits.

To conduct such an analysis regarding the impacts of the local RoCoF measurements, a second SG is introduced in the AC side under study, which might resemble a couple of small generating units, connected to station 1 as seen in Figure 2-61. This new generator is characterized by a Power System Stabilizer (PSS) and Automatic Voltage Regulator (AVR), featuring an inertia constant (H) of 1 second. It is modeled with a rated capacity of 1000 MW and an operating set point at 0.4 per unit (pu). The machine is linked to the Point of Common Coupling (PCC) with a specified impedance, representing its electrical distance from the PCC. Similarly, the bulk power system, represented by a Center of Inertia (COI), is also connected to the PCC with a designated equivalent impedance. Varying the values of electrical distances allows for an exploration of impedance's role in influencing local RoCoF measurements. The proposal to build this simulation scenario is to understand the local RoCoF behavior in both synchronous machines according to different operating points and grid conditions. Then, even if the scenario created is not plausible, it is useful for understanding the behavior of the local RoCoF.

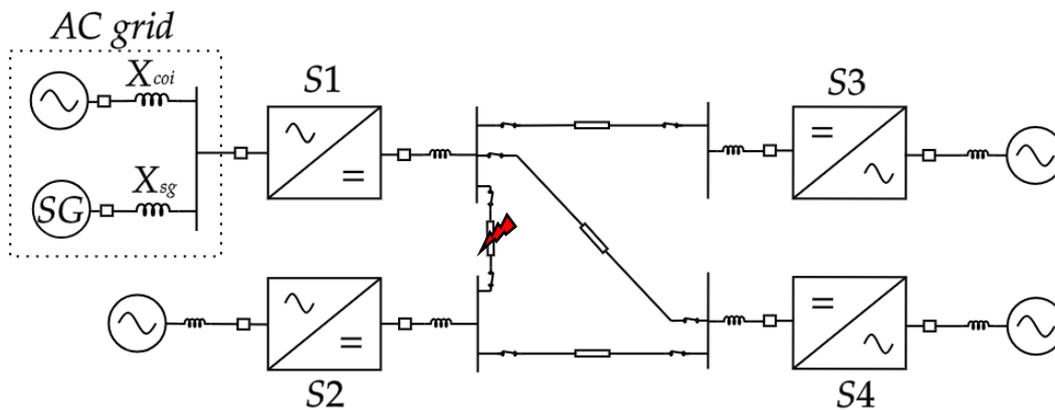


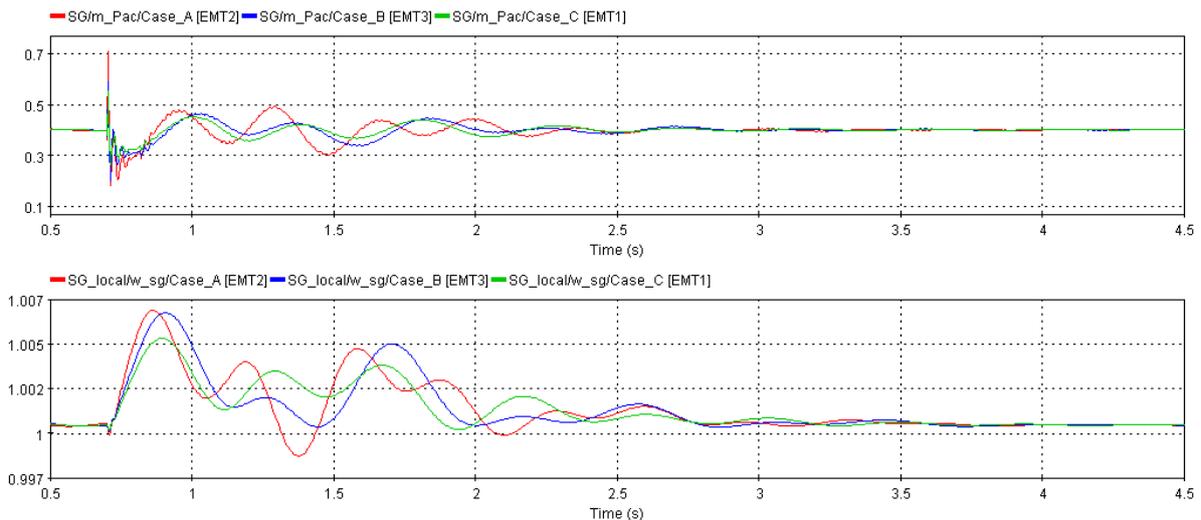
FIGURE 2-61: AC GRID COMPOSED OF SYNCHRONOUS MACHINE AND BULK SYSTEM (COI) CONNECTED TO STATION S1.

The analysis of the RoCoF is carried out varying the electrical distance of the synchronous machines connected to the PCC. To illustrate this idea, three different cases of the electrical distances are introduced in Table 2-10, where the electrical distance and the corresponding calculated RoCoF for a sampling time of 100 ms are presented when a DC pole to ground fault occurs in the positive pole of the cable that connects stations S1 and S2 in the middle point.

TABLE 2-10: COMPARISON OF LOCAL ROCOF FOR COI AND SG IN 3 DIFFERENT CASES.

CASE	COI		SG	
	$X_{coi}$	RoCoF	$X_{sg}$	RoCoF
A	0.5 [pu]	0.18 [Hz/s]	0.2 pu	2.33 [Hz/s]
B	0.2 [pu]	0.20 [Hz/s]	0.2 pu	1.83 [Hz/s]
C	0.2 [pu]	0.24 [Hz/s]	0.5 pu	1.00 [Hz/s]

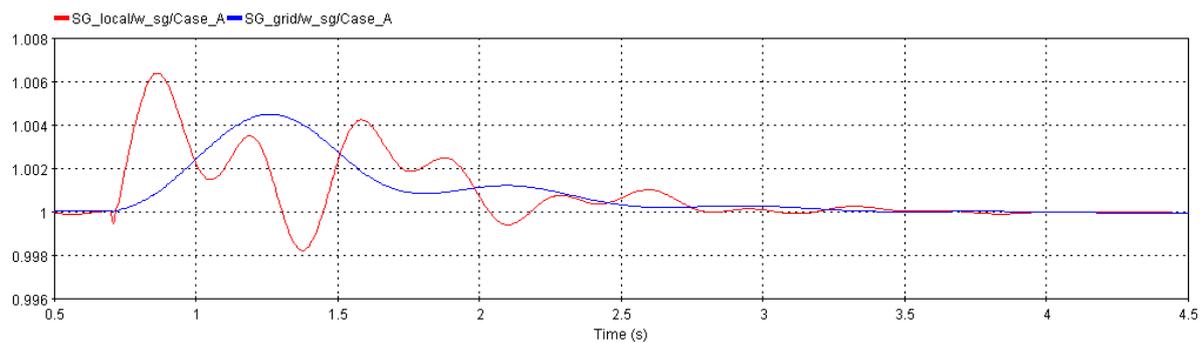
The active power output of the neighboring electrical machine and the frequency behavior of the COI and the SG for the three electrical distances are depicted in Figure 2-62. For case A, the SG exhibits a smaller electrical distance compared to the COI ( $X_{sg} < X_{coi}$ ), resulting in a higher acceleration of the nearest SG and a slower acceleration of the COI during a DC fault; the RoCoF calculated within a 100 ms time window is above 2 Hz/s, which might trigger some frequency protection actions at the local level in the SG depending on the duration of this situation [33]. Consequently, this machine experiences a larger initial swing, reflected in its output power and frequency, reacting to the power imbalance where the other machine and the converters in GFM participate in frequency support. In case B, both the synchronous machine and the center of inertia have the same equivalent impedance, where the rated power of the machine dominates over the dynamics of frequency, since the machine with higher capacity will respond to the power imbalance providing more power than the smaller machine; nonetheless, the RoCoF reached by the SG is about 1.8 Hz/s, which is close to the limits established for RoCoF requirements. Thus, the variation of the operating point in the SG might lead to reach this protection threshold, meaning that there is still a high influence of the DC fault in the local SG. Lastly, in the case C, the SG is farther from the point of common coupling when compared with the COI, therefore, the reaction of the SG to the system imbalance (DC fault) is reduced, since there is a big impedance between the SG and the PCC. So, it is expected that the local RoCoF of the SG is considerably decreased, being in this case close to 1 Hz/s.



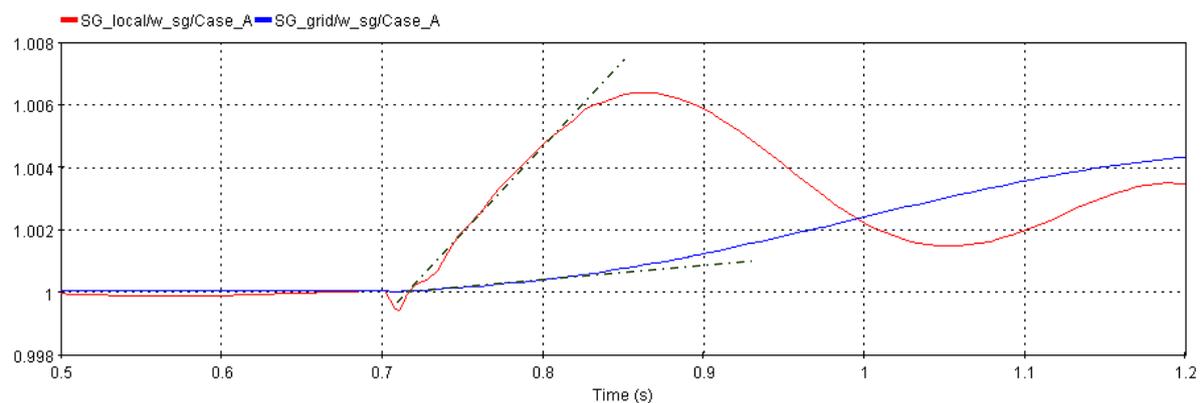
**FIGURE 2-62: ACTIVE POWER AND FREQUENCY CONSIDERING THE SG AND THE BULK SYSTEM.**

Another aspect considered in rotating machines is the behavior of the instantaneous settings of different frequency-based relays, since this is considered by protection schemes that might be configured on this mode for a particular application region [34]. Therefore, a comparison of the frequency responses and their respective RoCoF values of the COI and the nearest SG, for case A, are depicted in Figure 2-63. Nevertheless, it is worth mentioning that frequency protection relays have their own frequency estimation methods and filters. These tend to have longer calculation windows (three cycles for frequency estimation or more for RoCoF). Using the raw frequency from COI and SG are only used to provide insights on how the RoCoF measurement could use measurements from local equipment, but they may not represent the same frequency calculated by the relays.

As expected from the temporary loss of a rectifying converter, the neighboring SG will accelerate, in this case reaching a frequency deviation of above 0.2 Hz in 100 ms after the DC fault inception. In a similar manner, the bulk grid will experience an acceleration, yet, significantly lower, which leads to a smaller frequency deviation than that of the nearest SG, as seen before. This differentiated RoCoF between the local machine and grid's COI values is highlighted in the instantaneous calculation presented in the second graph of the same figure. These results illustrate the disparate behavior of frequency within the grid and the larger impact on nearby synchronous generators. Moreover, the RoCoF calculation might be done based on the frequency sampled measurements, ranging from an “instantaneous” value to hundreds of ms sampling rate, as presented in Table 2-10. Thus, a zoom into the frequency behavior is presented in Figure 2-64, this overview permits the graphical identification of the RoCoF when a sampling of 100 ms is used. The calculated RoCoF of the bulk grid in the first 100 ms is 0.18 Hz/s, whilst for the local RoCoF of the near SG is 2.33 Hz/s. This increased impact has consistency in both the continuous and the sampled calculation. Therefore, further sampled values will lead to other calculations in a similar pattern, having the first calculation as the one with the largest in magnitude.



**FIGURE 2-63: FREQUENCY VARIATION FOR THE SG AND THE BULK SYSTEM IN CASE A.**



**FIGURE 2-64: ZOOM IN THE SG AND BULK SYSTEM FREQUENCY TO BETTER UNDERSTAND THE ROCOF VARIATION IN BOTH SYSTEMS.**

During DC faults, an imbalance in power occurs within the AC grid, leading to system-wide frequency variations. However, each generator responds differently locally, depending on its electrical distance. Therefore, generators with shorter electrical distances exhibit a more pronounced impact on local RoCoF, indicating a stronger response compared to those with greater distances.

The significance of local RoCoF lies in its potential to trigger protection mechanisms based on local frequency measurements, possibly resulting in unforeseen generator disconnections within the grid. Consequently, local RoCoF proves to be a relevant metric for evaluating the repercussions of DC faults.

## 2.4. Power Electronic Grid Scenario

Throughout history, power systems operated on synchronous machines that rotated in synchrony, sharing power to meet demand, and offering inherent inertia (frequency response) to manage disturbances or shifts in operating conditions. Simulation tools and analysis methods evolved to accurately model and evaluate such systems. However, the traditional setup is becoming less accurate due to the widespread use of power electronic devices such as converters and modern loads. Many grids are evolving from ones whose dynamics are primarily defined by the electromechanical properties and characteristics of high-inertia rotating machines to ones primarily defined by power electronics controllers.

Wind, solar PV, PV, HVDC, grid support devices (STATCOMs, flywheels etc) and energy storage devices forming the main generation resource of PE-based grids, primarily employ power electronic interfaces for generation, but also for loads. Unlike conventional synchronous generators, these power converters lack inertial response due to the absence of rotating masses. The dynamic characteristics

of conventional grids are determined by the electromechanical properties of the directly coupled synchronous generators and their associated controllers. Power converters partially decouple the grid from the energy resource, so the dynamic characteristics are more heavily influenced by the design of the converter controller. To date, the vast majority of these converters have been designed to follow the grid rather than more actively contribute to frequency control and stabilisation. This has resulted in the need to introduce new methods to regulate frequency and to stabilise grids against undamped oscillations. Initially, the converter controller design struggle to naturally adapt to changes in load, deteriorating the frequency response and causing operational issues such as oscillations and reduced margins. Hence, the integration of inverter-interfaced resources has directly correlated with declines in inertia in many power systems. In nowadays applications, power converter controller design can allow us to pick and choose the valuable characteristics of conventional synchronous generator grids but applying creative engineering solutions to produce a more reliable, efficient, and stable grid.

As the grid transitions from a traditional generator-based model to one dominated by converters, the lack of inertia becomes a relevant concern in system operation and stability. Numerous remedies have been proposed, including the incorporation of energy storage and various grid-forming control strategies. Among these solutions, the concept of virtual inertia stands out—employing power converters that emulate synchronous machines. This approach offers a familiar framework for integration into the power network, contrasting the reserves of rotating masses (inertia) and damping windings in traditional synchronous machines, which help alleviate severe oscillations and enhance system stability.

In the context of HVDC-wise project, it's crucial to consider the implications of grid modernization by incorporating the scenario of PE grids. This inclusion allows for an analysis of the effects of DC faults, specifically regarding the reduction in inertia and the frequency dynamics unique to this type of system. Therefore, the PE grid scenario comprises a GFM converter that signifies the grid interconnection within a bipolar MTDC, alongside a GFL converter representing connections to renewable sources.

This case represents the interconnection of different Power Electronic (PE) grids using grid-forming (GFM) within VSM and grid-following (GFL) strategies as depicted in Figure 2-66, where the MTDC grid is composed of 4 bipolar terminals in minimum meshed configuration. The converters in stations S2, S3 and S4 are in Vdc-mode (DC voltage control). The station S1 is configured in GFM control with P-mode (power control), they are connected in the AC side with 2 power converters, the first in a 2000 MVA station in GFM (VSM with frequency droop) giving the frequency reference and the second is 1000 MVA nominal power in GFL control. They are connected in 400kV grid. An impedance between the station S1 and converters can represent the electrical distance of those grids (SCR = 1.9 weak grid scenario). In this case, the non-selective protection scheme is chosen since it may lead to higher stability impacts for the AC grid. The converters in station S1 are also in GFM control, named Pos\_S1 and Neg\_S1.

The PE\_GFM converter can represent various converters within the GFM, characterized by their inertia constant and frequency droop constant and the PE\_GFM converter represents in the integration of renewables, e. g. Offshore Wind Farms (OWF). The sum of the PE\_GFM and PE\_GFL converters will compose the PE grid. This setup enables the exchange of power between the bipolar MTDC and the AC grid, operating under the principles of the virtual inertia paradigm. This arrangement facilitates a more comprehensive understanding of the repercussions of significant disturbance events. To assess angle and frequency stability, the PE grid scenario is structured to undergo EMT simulations. This approach allows for an in-depth analysis of the stability aspects within this context.

The frequency droop is inserted only in the GFM converter in the left that composes the PE grid, by a power reference as presented next:

$$P^* = P_{ref} - K_{\omega}(\omega_{vsm} - \omega^*) \tag{2.8}$$

where  $P_{ref}$  is the desired power to be dispatched in the converter (given from a higher control layer to provide power balance in the AC grid),  $\omega^*$  is the frequency reference and the droop gain is given as  $K_{\omega} = 80$ . Station S1 in the MTDC grid has no frequency droop implemented.

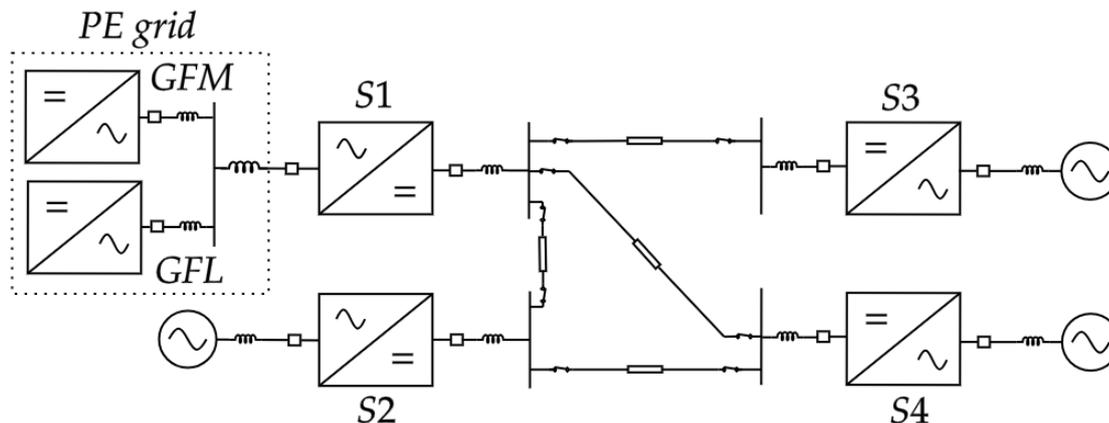


FIGURE 2-65: ELECTRICAL MODEL OF THE PE GRID (GFM+GFL) CONNECTED TO THE MESHED MTDC GRID.

The configuration of GFL converter that composes the PE grid and the converters from the MTDC link are detailed in Table 2-5 from reference simulation section. The GFM converter of the PE grid is modelled with parameters adjusted to have 2000 MVA of nominal power, which is also adjusted to its per unit transformation. The initial power flow in the AC side is defined and presented in Table 2-11 and the power flow in the MTDC is presented in Table 2-12, where negative values designate power injected into the DC grid.

TABLE 2-11: INITIAL POWER FLOW IN AC GRID FOR THE PE GRID.

CONVERTER	P	Q
PE_GFM	1600 MW	400 MVar
PE_GFL	200 MW	0 MVar
Pos_S1	-900 MW	300 MVar
Neg_S1	-900 MW	300 MVar

TABLE 2-12: INITIAL POWER FLOW IN THE MTDC FOR THE PE GRID.

CONVERTER	P	Q
Station S1	-1800 MW	600 MVar
Station S2	1800 MW	400 MVar
Station S3	-800 MW	400 MVar
Station S4	800 MW	400 MVar

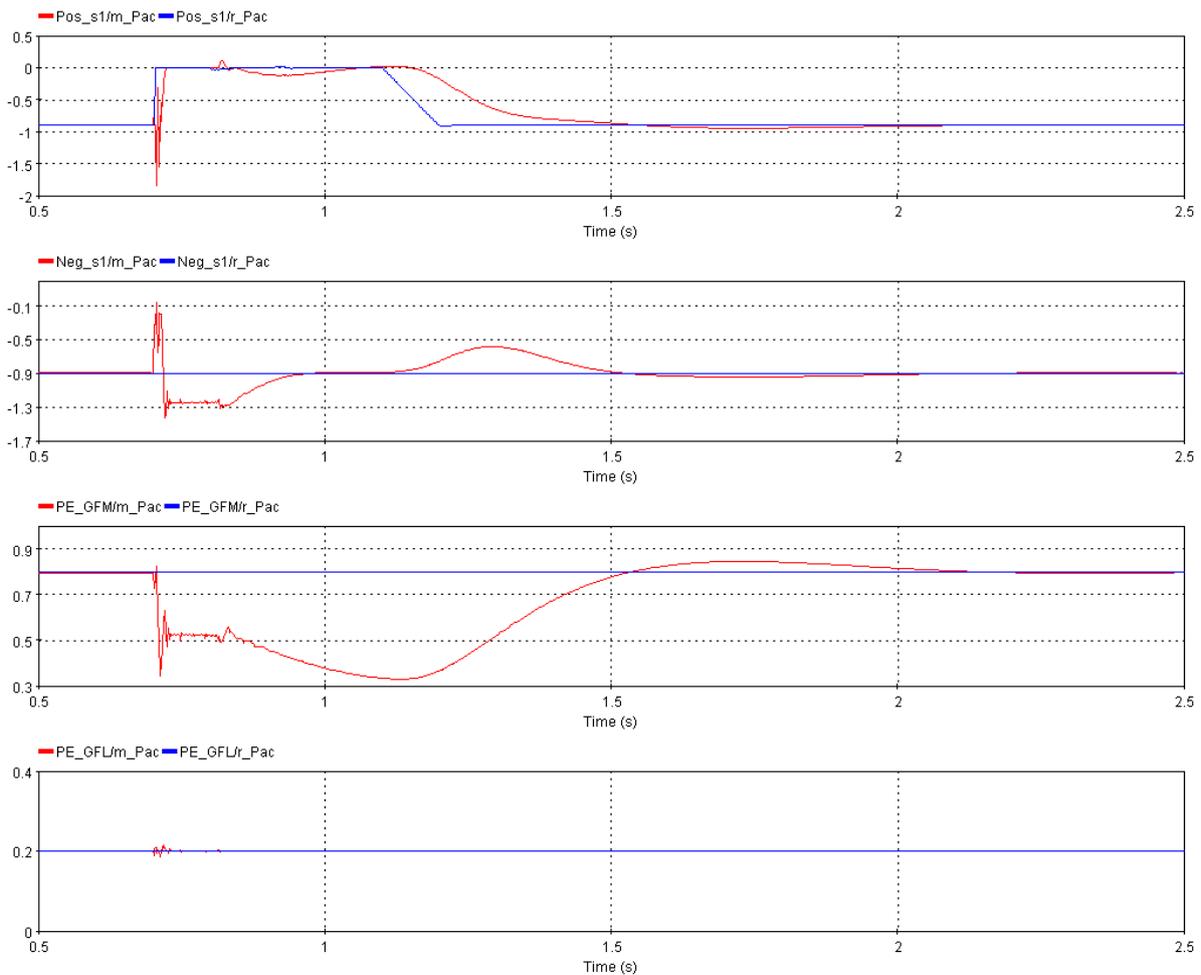
The protection sequence in this case is done according to Figure 2-3.

### 2.4.1. DC Fault (pole to ground)

The investigation of the DC fault first analyzes the power profile of the converters in the AC grid connection as depicted in Figure 2-66. The DC fault is also located at the midpoint of cable that connects the stations S1 and S2, similarly to previous simulations. At the moment of the DC fault, the positive pole (Pos\_s1) has a power spike, injecting 1.67 pu power into the DC grid to supply the fault. At the same time, the negative pole (Neg\_s1) and the GFM converter (PE\_GFM) have a power peak, reducing the power supply to -0.1 pu and the 0.33 pu, respectively, in the opposite direction of Pos\_s1. Thus, both converters act counteracting the DC fault by injecting power into the AC to assure the system balance. Once, the DC breaker is opened (at 0.710 s), the power goes to zero in the faulty pole (Pos\_s1), and the healthy pole (Neg\_s1) reacts absorbing power to balance the power flow, where the current limitation is activated maintaining the operation of the healthy pole limited to -1.3 pu. Therefore, the GFM converter (PE\_GFM) provides the needed power to the healthy pole to assure power balance, considering the limited power of the healthy converter.

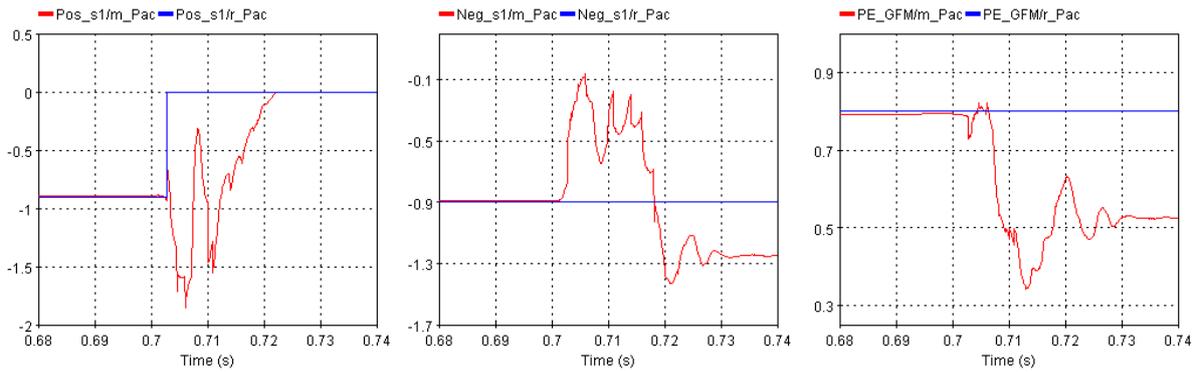
Next, the faulty cable is isolated, and the faulty converters are deblocked at 0.815 s of simulation. The DCCB is reclosed at 0.930 s, in this meanwhile the reactive power is restored at 0.830 s. It is possible to notice that right after the converter is deblocked, the faulty pole (Pos\_s1) reacts to the activation of the energy control loop using AC power, which causes a small power transient. The other converters, Neg\_S1 and PE\_GFM, also react due to the Pos\_S1 deblocking, where the healthy pole follows again its power reference and the PE\_GFM converter provides the required power to supply the system with slower dynamics. This behavior of reacting to power imbalance comes from the swing equation implemented in the grid forming strategy. Which means that power reference changes and frequency perturbation will cause a transient response called inertial support. That is why the GFL converter (PE\_GFL) is not considerably disturbed during the fault, and it does not represent a significant influence on the system's dynamics.

It can be noticed from Figure 2-66 that the PE\_GFM converter is not following its reference during the DC FRT to precisely assure the power balance in the system. This is done by introducing a frequency droop term from (8) in the power reference of the VSM swing equation, so the steady state frequency is controlled mainly by the GFM converter (the frequency droop is not inserted in the other converters). The droop gain is given here as  $K_{\omega} = 80$  and the frequency reference is given in per unit  $\omega^* = 1$ .



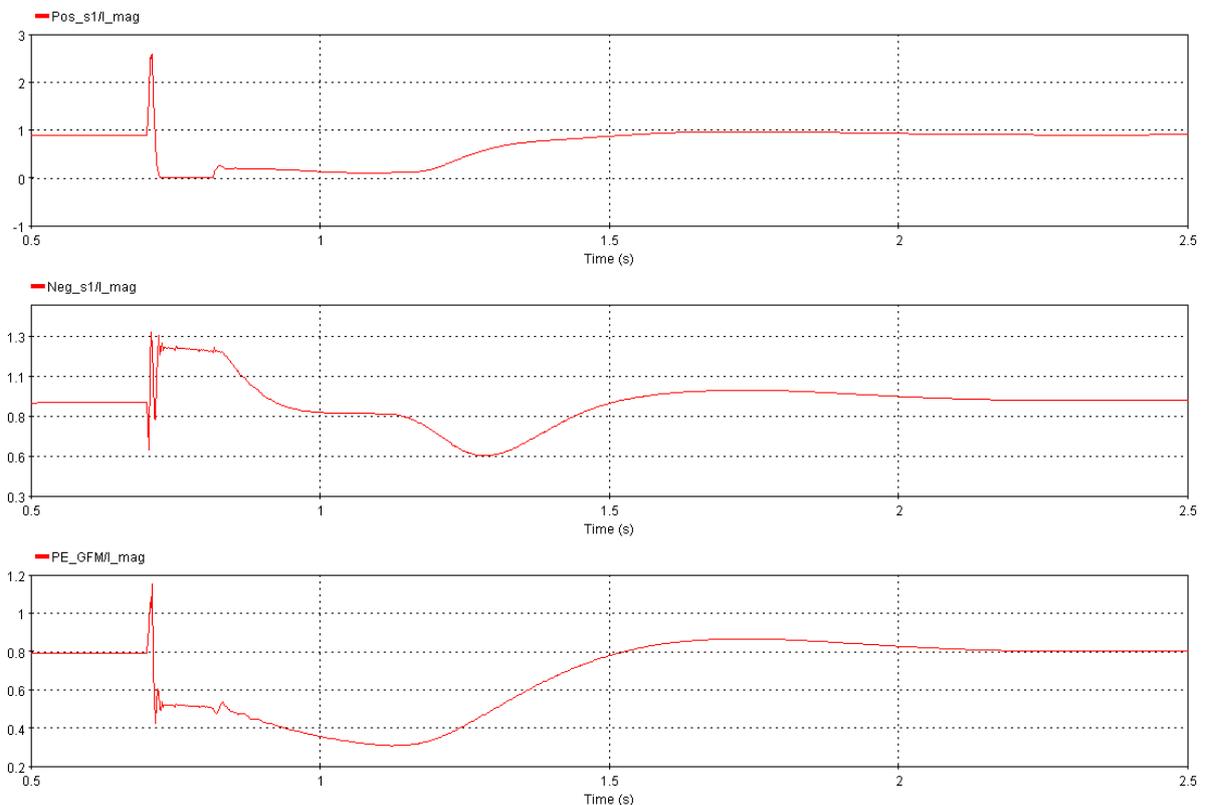
**FIGURE 2-66: ACTIVE POWER PROFILE IN PE\_GFM, PE\_GFL, POS\_S1 AND NEG\_S1, AND THEIR REFERENCES.**

A zoom in the power profile of the station S1 and the PE\_GFM is depicted in Figure 2-67 to better show the transients at the moment of the DC fault. Once the Pos\_s1 converter is blocked, the swing equation of the faulty converter is deactivated, which means that the phase angle value applied to the converter has no power action in the control until the converter is deblocked. When the converter is deblocked, the VSM control block is reset, considering the PLL values (grids' phase angle and frequency) as the initial values. Also, the active power reference is set to zero while the converter is blocked, activating the external energy control loop when is deblocked, balancing the internal energy of the faulty pole by the AC grid side. Once the DCCB is reclosed, the active power is restored at 1.1 s, presenting a smooth and slow transient for active power in both poles of station S1 but also to the GFM converter of the PE grid, where the original equilibrium point is again obtained.



**FIGURE 2-67: ZOOM IN THE ACTIVE POWER PROFILE IN PE\_GFM, POS\_S1 AND NEG\_S1, AND THEIR REFERENCES.**

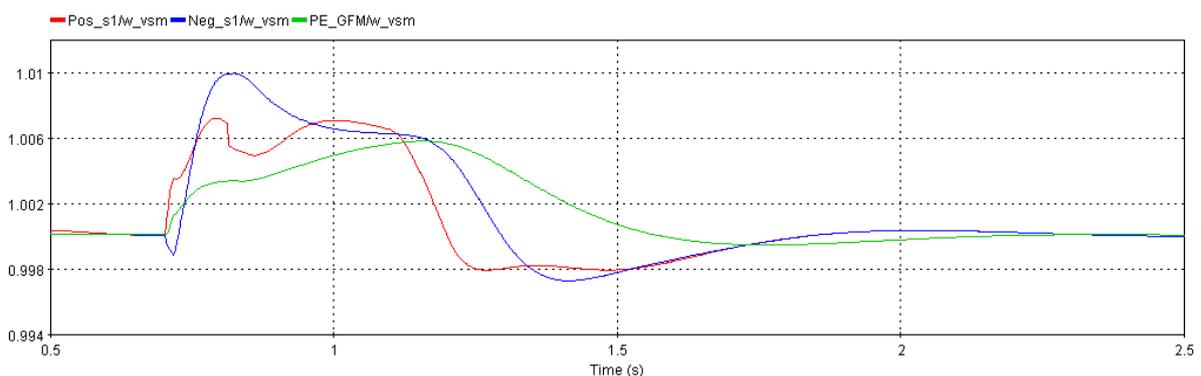
The current magnitude profile of the station 1 and the PE\_GFM converter are presented in Figure 2-68. The current can better describe the behavior of each converter regarding the actions of the GFM control since the AC voltage is more affected in this case when compared with the other AC grid architectures (weak grid and synchronous machine grid). Initially, when the DC fault occurs, the positive pole has a peak of current to supply the DC fault, then going very fast to zero once the DCCB is opened. The PE\_GFM converter also has a peak providing current to the fault and then reducing the current level to supply the remaining converter in operation (Neg\_S1). On the other hand, the healthy pole initially reacts counteracting to the DC fault, reducing the current level, and right after, when the faulty converter is blocked, the Neg\_S1 reacts to this phase jump (created when the faulty converter is blocked) by increasing the current supply until the limits (at this point the current limitation is activated in the Pos\_S1 converter). Once the faulty converter is deblocked, the healthy converter reduces its current profile to its reference. In this case, it is much simpler to identify the GFM behavior in the currents profile.



**FIGURE 2-68: CURRENT MAGNITUDE IN POS\_S1, NEG\_S1 AND PE\_GFM CONVERTERS.**

In a PE grid, the frequency is obtained from the virtual swing equation of the converters, producing the calculated VSM frequency for each converter. The frequency produced by the converters in grid-forming are introduced in Figure 2-69. Initially, the frequency of the Pos\_S1 converter is temporally reduced due to the inertial response of the GFM control since it is the closest converter to the DC fault. While the frequency of the PE\_GFM converter increases reacting to the loss of power infeed from the Pos\_S1 converter, its action to the DC fault is not substantial. Once the faulty converter is deblocked, the Pos\_S1 is relieved, reducing its frequency, while the frequency of PE\_GFM increases with very slow dynamics. Finally, when the DCCB is reclosed and the active power is restored, the frequency of all converters has a last transient returning to the original equilibrium point, since the power of the faulty converter is retaken.

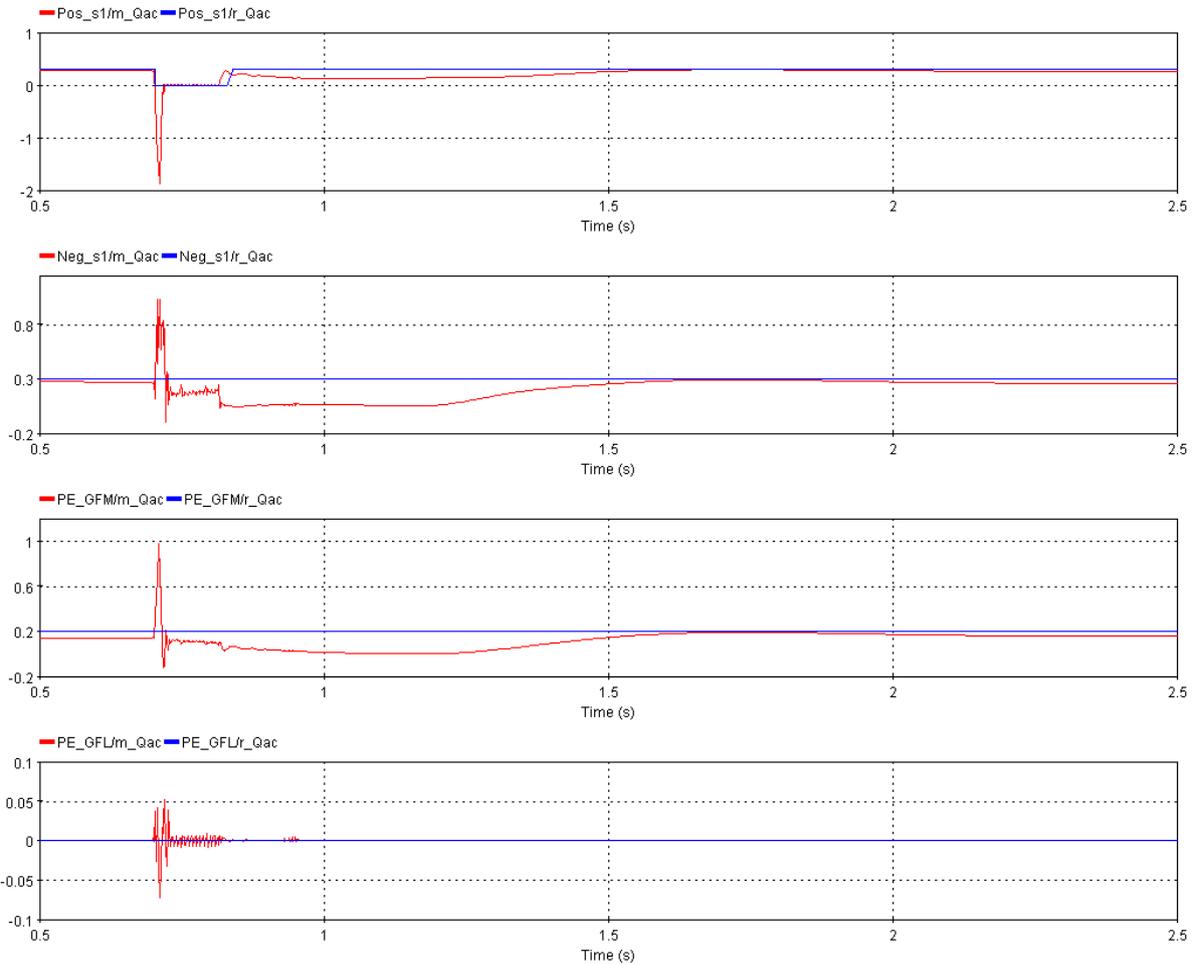
The RoCoF in the healthy pole (Pos\_S1) is higher than the one in the PE\_GFM converter, both for the initial transient of the fault and during the restoration of active power. This can be explained because of the electrical distance between Pos\_S1 and PE\_GFM converters regarding the point of the fault. The positive pole is much closer to the fault compared with the PE grid converter due to the high impedance between the PE\_GFM converter and the PCC. Also, the droop control of the PE\_GFM converter changes the dynamics of the frequency in the swing equation, then we can see slower dynamics for the PE grid converter.

**FIGURE 2-69: VSM FREQUENCY DYNAMICS IN PE\_GFM, POS\_S1 AND NEG\_S1.**

The reactive power profile of the station S1 and the PE grid converters are depicted in Figure 2-70. This case is very similar to the previous cases, e. g. the weak grid scenario in GFM control. The converters of the PE grid (Pos\_S1, Neg\_S1 and PE\_GFM) are sharing the AC voltage control, therefore when the DC fault happens, the voltage of the Pos\_S1 converter will be drastically reduced, absorbing a huge amount of reactive power (close to 2 pu). While the negative pole and the PE\_GFM converter will react to maintain the voltage on the PCC by injecting a peak of reactive power to the AC grid, both converters provide close to 1pu of reactive power. Once the faulty converter is blocked, its reactive power reference is set to zero and the measured power also goes to zero. The healthy converter activates the current limitation during this same period, so the reactive power is limited close to zero.

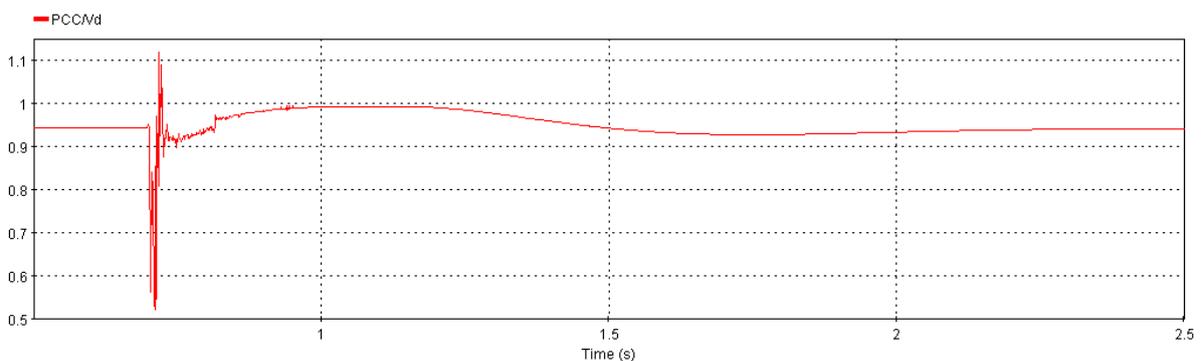
When the faulty converter is deblocked, the reactive power is reactivated by the AC voltage droop control, sharing the voltage control among the converters. At this moment, the AC voltage control is shared by all converters in the grid (except the GFL converter), and as the active power has a different setpoint (given by the DC FRT operation), there is a new equilibrium point of reactive power, which is much smaller than the pre-fault condition. That is why, the period in between the converter deblock and the active power restoration, the level of reactive power in the system is quite reduced. After the

active power restoration, the reactive power is increased back to allow the power transfer in the AC grid.



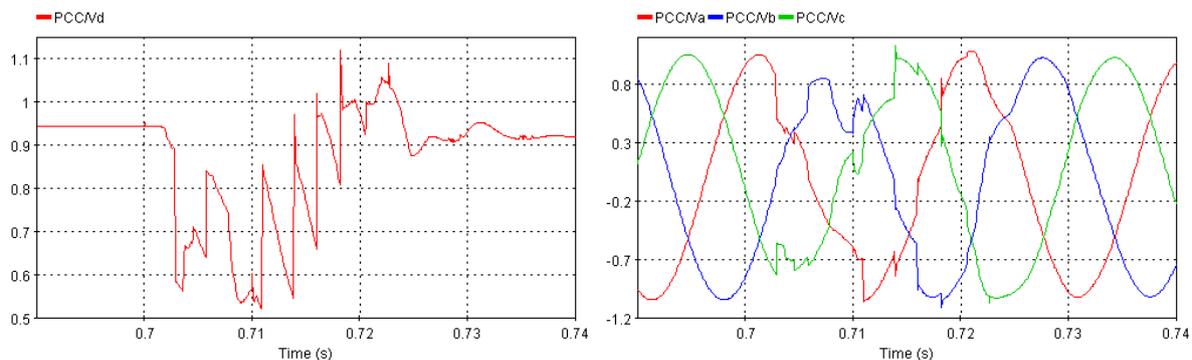
**FIGURE 2-70: REACTIVE POWER PROFILE IN THE PE GRID.**

Figure 2-71 illustrates the AC voltage magnitude at the PCC. Initially, there's a noticeable drop in the AC voltage, followed by its recovery to acceptable levels upon opening the DCCB. Once the converter is deblocked, the AC voltage control is retaken, enhancing the voltage profile behavior. During the period between converter deblocking and DCCB reclosure, the AC voltage level rises above the pre-fault condition. This occurs because the system's active power supply has significantly decreased, requiring less reactive power to maintain voltage levels. When active power is restored, the AC voltage returns to its original operating point.



**FIGURE 2-71: AC VOLTAGE MAGNITUDE AT THE PCC CONSIDERING THE PE GRID.**

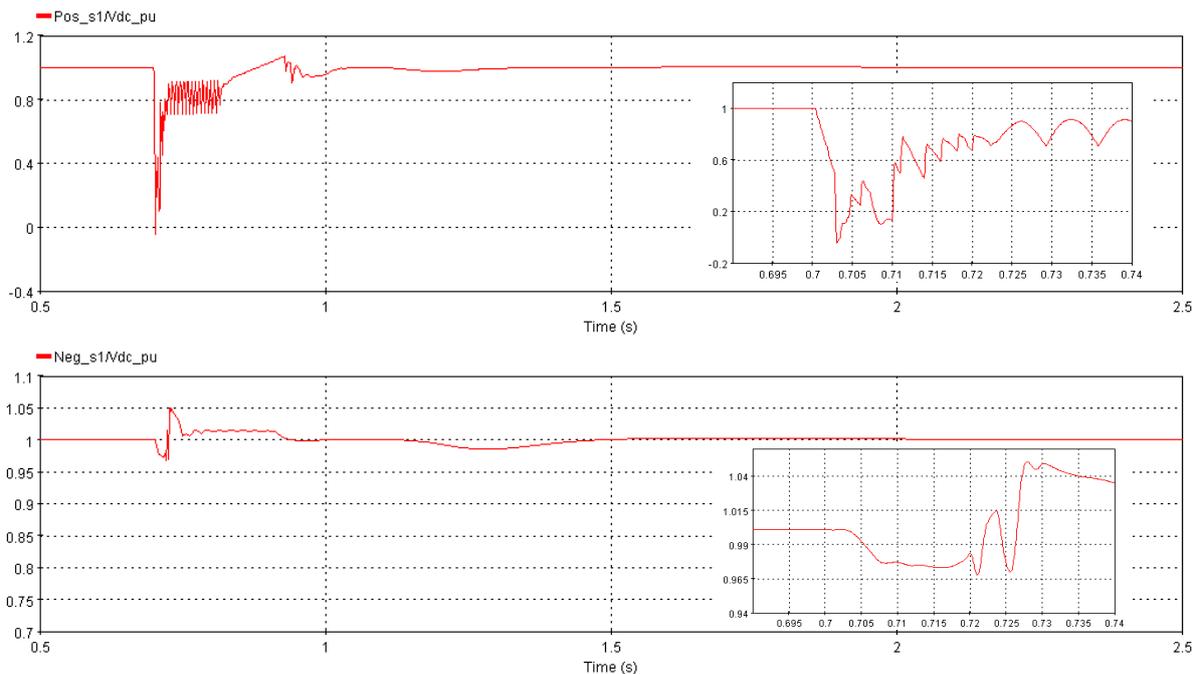
Figure 2-72 provides a detailed view of the AC voltage magnitude and the three-phase voltage signal during the occurrence of a DC fault. At approximately 0.703 s simulation, there is a significant decrease in voltage immediately after the faulty converter is blocked. Subsequently, upon opening the DCCB, the voltage is quickly restored to reasonable levels with an oscillatory pattern. Concurrently, the three-phase voltage signal experiences a brief disturbance within the initial 10 ms of the DC fault, swiftly returning to its characteristic smooth sinusoidal waveform.

**FIGURE 2-72: ZOOM IN THE AC VOLTAGE MAGNITUDE AND THREE-PHASE WAVEFORM DURING FAULT TRANSIENT.**

Now, the DC voltages on the positive and negative poles of station S1 are introduced in Figure 2-73. One notices that the DC voltage on the positive pole goes quickly to zero when the DC fault takes place, mainly after the converter blocking. Then, once the DC breakers are opened, it works in rectifying mode until the converter is deblocked at 0.815 s. After the MMC deblocking, the DC voltage quickly rises close to 1.6 pu/s, being controlled by the external energy control loop that regulates the internal energy of the converter, assuring the stability of the DC voltage. As the power balance is assured (sum of power in the MTDC is zero), the DC voltage reference is exactly 1 pu.

The DC voltage on the negative pole experiences a small transient during the DC fault event, while the Neg\_s1 pole has an overshoot of 0.09 pu in the transients, which is considered inside of the limits to avoid protection actions established on the simulations (The protection actions are triggered from overshoots of 10% in a time greater than 50 ms). During the fault, the DC voltage increases to 1.05 pu, because the power flow is changed during this time (an unbalance of 800 MW is produced when the Pos\_s1 is blocked).

Once the DCCB is reclosed, the system has a small transient, and the voltages follow their references again, where the faulty pole presents higher transients compared with the negative pole. It should be noted that the converters in GFM control in the MTDC are controlled in P-mode, which means that the converters in GFM must have a strategy to control DC voltage during the DC FRT, where in this case the external energy control loop is applied. So, to avoid DC voltage instability in the GFM station (S1 and S2), the DC voltage control must be guaranteed by the MTDC link.



**FIGURE 2-73: DC VOLTAGE POSITIVE AND NEGATIVE POLES OF STATION S1 CONSIDERING THE PE GRID.**

### 2.4.2. Oversizing the Converters

In this subsection an oversized bipolar station in GFM is analyzed considering the PE grid interconnection. As in previous cases, the converters in station S1 have increased the capacity of 20% regarding nominal power (current capacity is proportionally increased). It is carried out to enlarge the available headroom to provide the expected services to the AC grid in case of a disturbance, e. g. frequency and voltage support, while having a nominal full capacity output of 1000 MW. This proposition is expected to enhance the stability of the AC system, while operating at the previous nominal full capacity, which might not be reached with a regular size, since headroom is normally considered to avoid congestion in peak hours, N-1 contingencies or larger contingencies in the AC grid that might require the spared capacity. It is investigated if the impacts on the AC grid side during the fault are reduced, what could justify the investment to increase the converters in the MTDC.

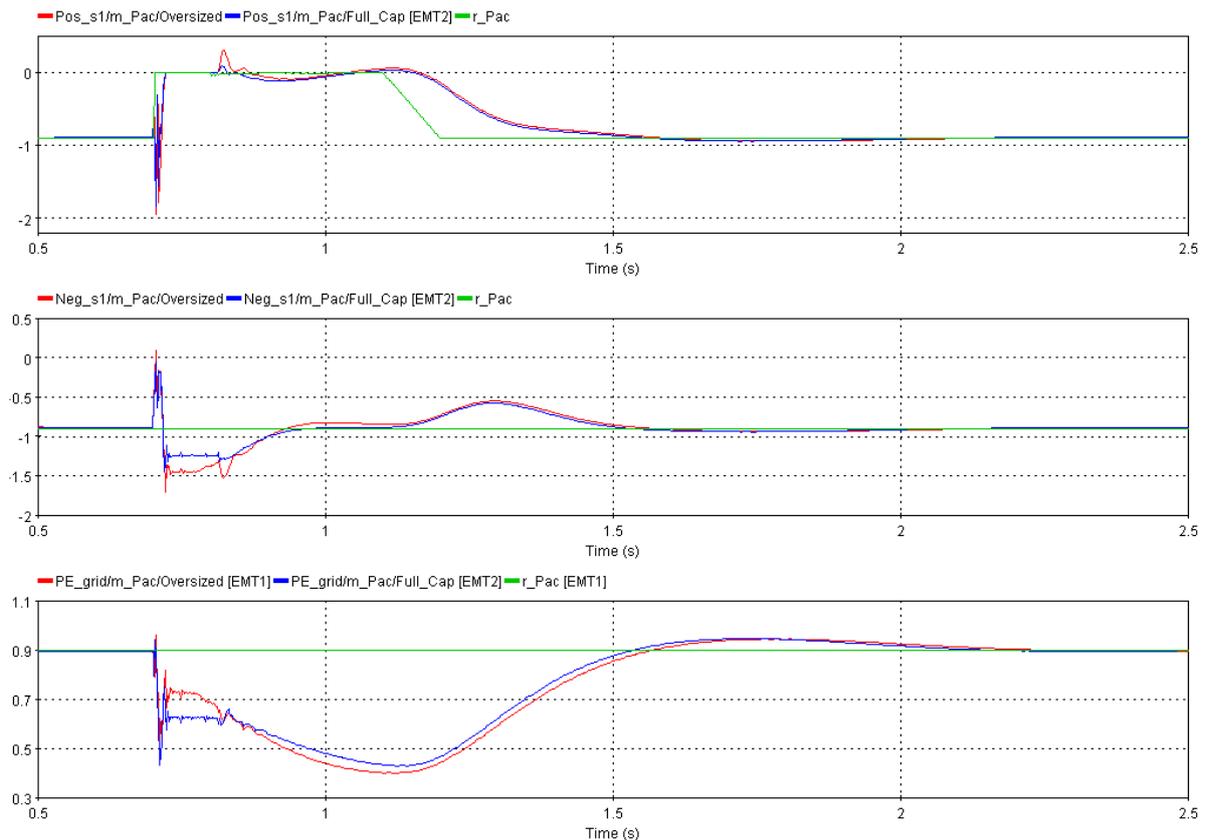
In this case, the GFL converter is set to zero to establish a critical operating point to the GFM converter in the PE grid, where the power references are close to the operational limits. The initial power flow in the AC side is defined and presented in Table 2-13 and the power flow in the MTDC is applied according to Table 2-12.

**TABLE 2-13: INITIAL POWER FLOW IN AC GRID FOR THE PE GRID.**

CONVERTER	P	Q
PE_GFM	1800 MW	400 MVar
PE_GFL	0 MW	0 MVar
Pos_S1	-900 MW	300 MVar
Neg_S1	-900 MW	300 MVar

The protection sequence in this case is done according to Figure 2-3 and the power base to perform the per unit transformation is kept the same for the oversized converter ( $S_{base} = 1000MVA$ ).

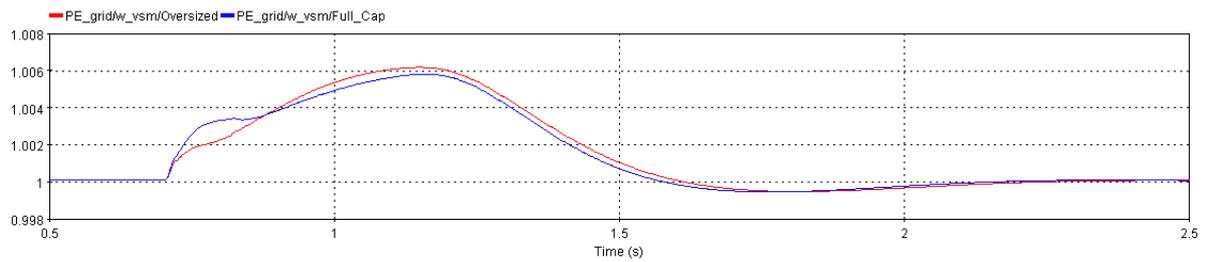
Figure 2-74 depicts the active power profile in the PE grid considering that the GFL converter is not supplying power, so only the GFM converter is supplying the demanded power to station S1. As in previous cases, the power reaction towards the DC fault has the earlier described behavior. Nonetheless, the healthy pole is able to supply a larger amount of power to support the AC side since current limitation is not triggered with the oversized converter. As in the reference case, the healthy converter has the largest participation in the power injection, due to the closest electrical distance to the fault. The action of the PE\_GFM converter is limited because of weak grid condition. Once the fault is cleared and the active power is restored, the power behavior of converters is quite similar even considering the oversized converts, which means that the oversizing contributes only is the operational limits of the system, therefore no difference is seen in normal operational conditions.



**FIGURE 2-74: ACTIVE POWER PROFILE IN PE\_GFM, PE\_GFL, POS\_S1 AND NEG\_S1, AND THEIR REFERENCES.**

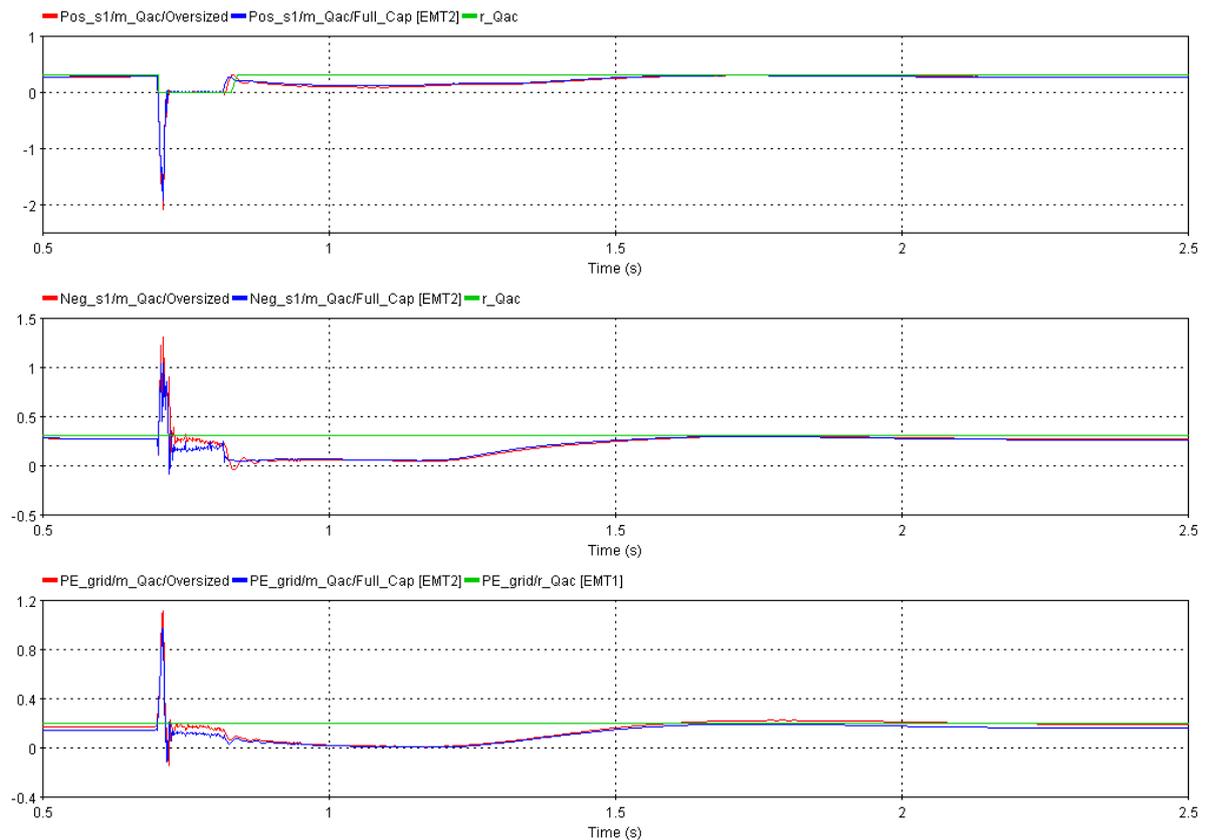
The VSM frequency of the PE\_GFM converter comparing the oversized and the original size converter is depicted in Figure 2-75. Due to the larger participation of the healthy converter to maintain the AC grid stability, the frequency has a slightly reduced acceleration after the initial transient. In the case of the oversized converter, as the current limitation algorithm remains inactive, the frequency variation of the PE grid after the initial is smoother. However, the maximum frequency deviation is slightly larger in the oversized case. This larger deviation arises from the fluctuation in power output from both converters, facilitated by their increased capacity, enabling larger power injections.

### D3.3: Protection Concepts



**FIGURE 2-75: VSM FREQUENCY DYNAMICS IN PE\_GFM, POS\_S1 AND NEG\_S1, AND THE MEASURED PLL FREQUENCY.**

The reactive power profile in the AC grid is portrayed in Figure 2-76. As expected for the oversized case, the reactive power injection is very close to reference case. The main advantage is only seen during the operation of current limitation in the converter with original size. Furthermore, the oversized healthy converter and the PE grid have larger power injections to maintain voltage levels on the AC grid when compared with the full capacity reference case. These injections are then reduced once the faulty converter is deblocked and its inherent STATCOM operation starts. Also, the increased capacity of the converter allows a smoother output profile after the MMC deblocking. Besides that, the impact of the AC voltage is minimum, implying an irrelevant difference for the behavior of the AC voltage. It is possible to state that oversizing the converter is not relevant to AC voltage control.



**FIGURE 2-76: REACTIVE POWER IN AC SIDE OF THE GRID AND THE VOLTAGE PROFILE IN THE PCC.**

A comparison of DC voltage at the positive and negative poles for the reference and the oversized cases is shown in Figure 2-77. The positive pole shows practically the same behavior until the deblocking of the faulty converter. During this time, the oversized converter takes a larger amount of power from the AC side, performed by the energy control of the outer loop, therefore reducing the

DC voltage overshoot after the MMC is deblocked. For the healthy converter the difference is minimum, despite the smaller DC voltage variations of the oversized converter. The DC side remains connected to the AC grid in the healthy converter; therefore, the DC grid is capable of maintaining a similar level to the one of the reference cases.

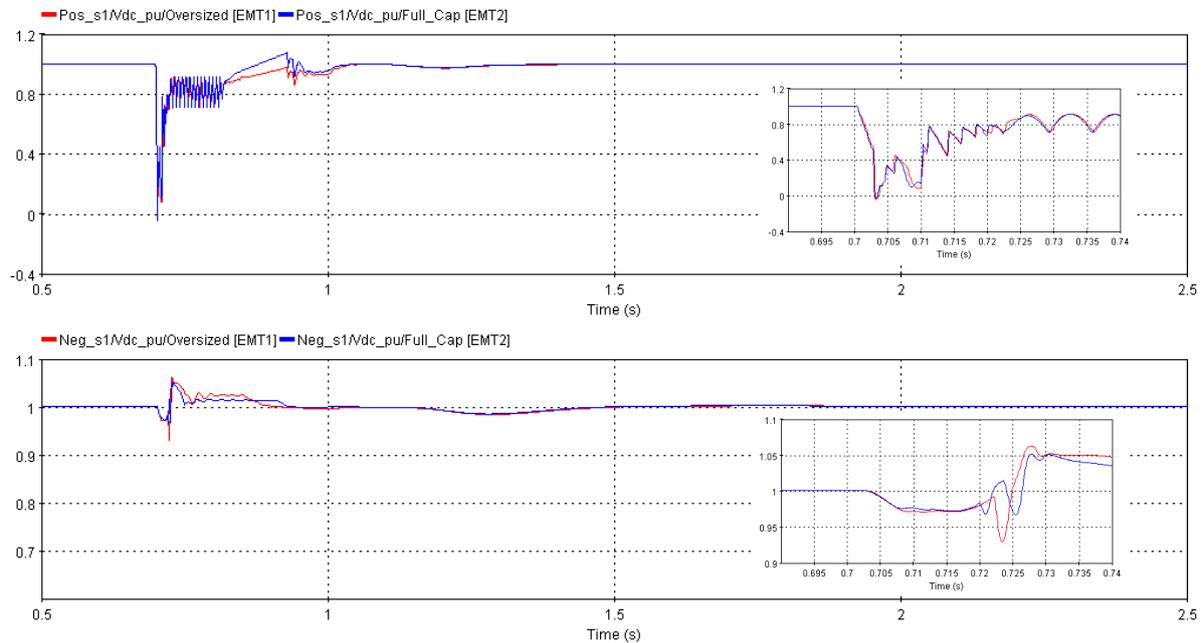
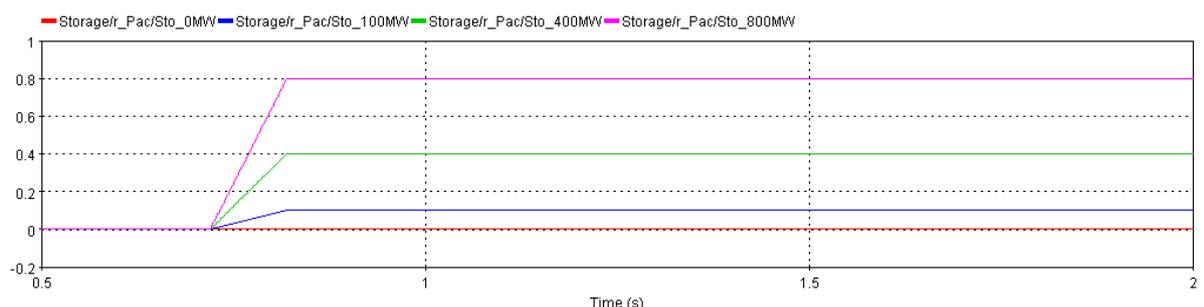


FIGURE 2-77: DC VOLTAGE POSITIVE AND NEGATIVE POLES.

### 2.4.3. Energy Storage Insertion

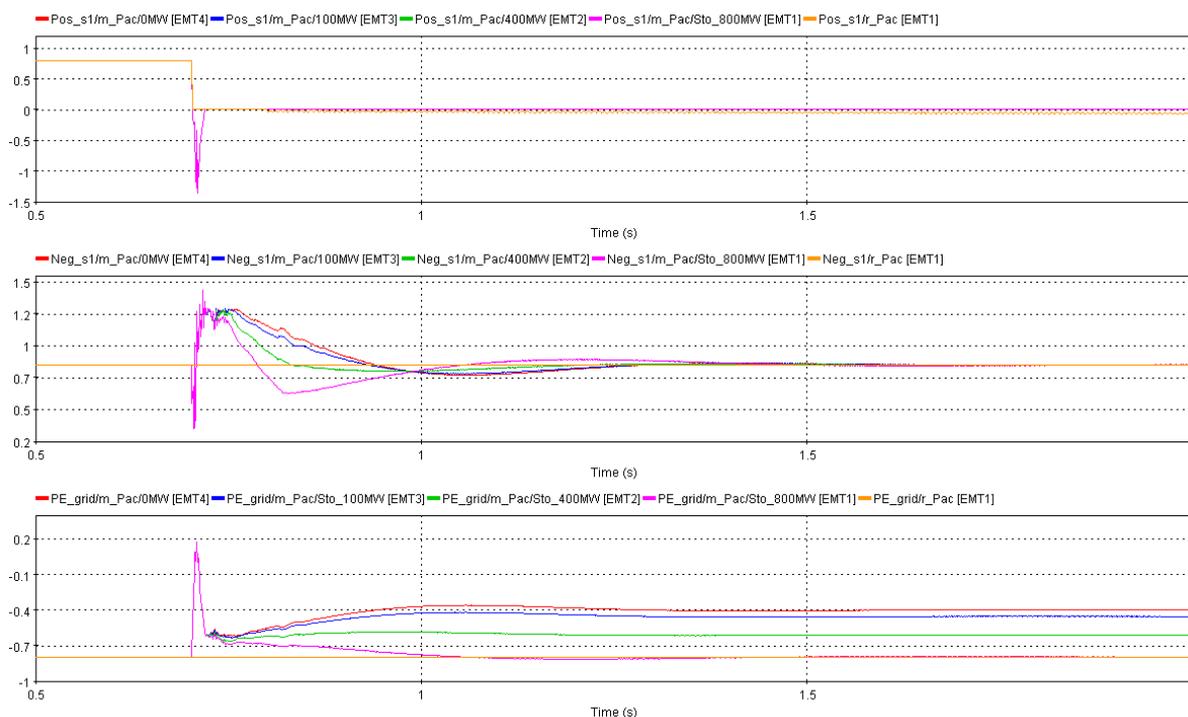
In this subsection, an energy storage system is connected in the AC side of the grid composing a new converter element. The energy storage is interfaced by a power converter which will dispatch power according to a given reference. The idea is to contribute to the power balance in the AC side when the system is disturbed by the DC fault, therefore the impacts in the AC grid should be reduced thanks to the available power in the energy storage system.

In this case, the energy storage system is connected in GFL mode, and it supplies power to the AC grid when there is a fault on the DC side of the grid. The storage is triggered to dispatch power at the moment of the DC breakers opening, considering a communication delay of 10 ms. So, the power reference in the battery is activated at 0.720 s of simulation and there is a 100 ms ramp to reach the desired reference. Three different scenarios have been tested according to the different power dispatch of the energy storage: 100 MW, 400 MW and 800 MW. The power dispatch in the energy storage system is shown in Figure 2-78, first with no storage being dispatched as the reference scenario, second with 100 MW, third with 400 MW and fourth with 800 MW dispatched.



**FIGURE 2-78: POWER DISPATCH PROFILE OF THE STORAGE IN THE AC GRID.**

The power profile of the AC side converters is depicted in Figure 2-79. The reference scenario is presented in red line, which represents the system response without the storage. The initial transient is similar in all cases, but as the power injection into the storage system increases, the phase jump power injection on the negative pole decreases, and the demanded power to be absorbed by the PE\_GFM converter is closer to the original reference (pre-fault value), which means that the system is less disturbed in the fourth case. The positive pole presents a similar behavior for all case scenarios since the storage does not affect the power of the faulty pole.



**FIGURE 2-79: ACTIVE POWER PROFILE CONSIDERING THE AC ENERGY STORAGE.**

The frequency and the AC voltage at the PCC are depicted in Figure 2-80 and Figure 2-81, respectively. We can clearly see that the frequency has the same initial RoCoF for all scenarios, since there is a time delay of 20ms in between the fault and the activation of the energy storage. So, if the energy storage system were required to provide inertial support, the best option would be to insert the storage system in GFM control or consider the activation of the storage according to RoCoF ratio limits (frequency support). But, as expected, it also can be noticed that the storage helps to improve the frequency nadir, since the storage system increases the power level supply in the AC side of the grid. This behavior can be seen as a secondary frequency control increasing the steady state value of frequency closer to its nominal value. The voltage profile is similar for all case scenarios during the initial transients, but the steady state voltage level is reduced as the power supply of the energy storage is increased, since the ESS increases the active power flow in the grid, requiring more reactive power to support this power exchange, as a response, the level of the voltage is degraded as the ESS supply increases. This characteristic is evident in the weak grid, when the operating point is close to the system's operating limits, where the injection of active power directly affects the AC voltage level.

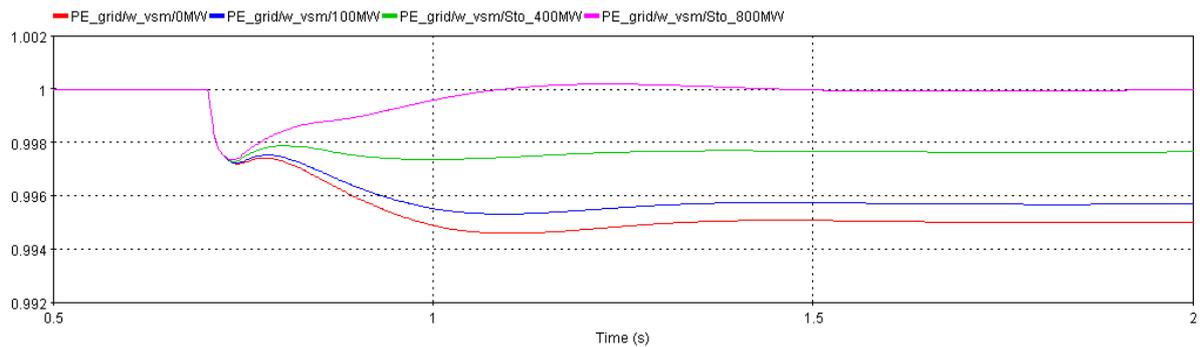


FIGURE 2-80: VSM FREQUENCY OF THE PE GRID CONSIDERING THE AC ENERGY STORAGE.

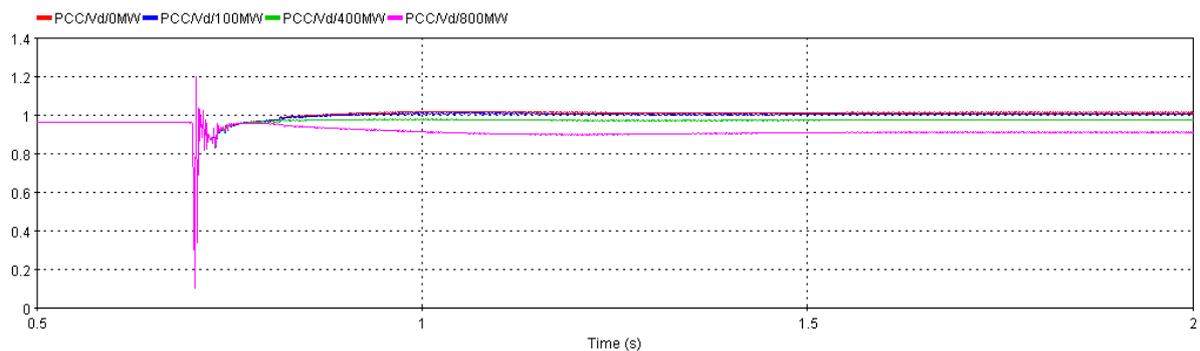


FIGURE 2-81: AC VOLTAGE ON THE PCC CONSIDERING THE AC ENERGY STORAGE.

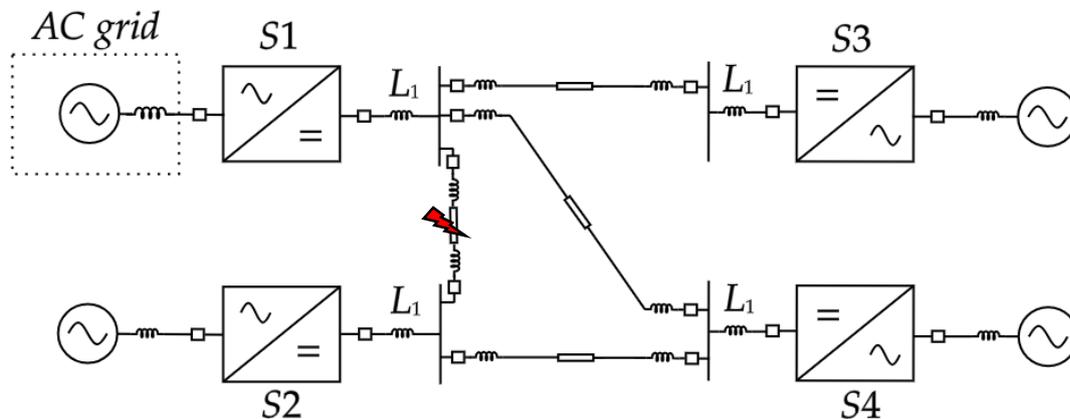
## 2.5. Fully Selective philosophy

In this subsection, the Fully Selective (FS) protection philosophy is taken into consideration regarding the GFL and GFM characteristics. The purpose is to analyze the impact of the FS philosophy in the DC FRT operation, where it is expected to result in minimum impact to the system operation due to the fast action of the DCCBs to clear the fault without disconnecting the whole grid, but only operating the DCCB closest to the fault in a selective manner. The MTDC then is transiently disturbed, where a new DC power flow is reached. The DC perturbation is propagated to the AC side as power transient. Therefore, when the converter station is in GFM control, the disturbance can be propagated to AC voltage and frequency. Thus, an analysis in these cases is carried out.

The electrical model of the FS philosophy is depicted in Figure 2-82. In this case, each line of the MTDC is installed with a DCCB at both terminals of the cable and a DC Reactor (DCR) to limit the rate of change and level of the fault current. Therefore, each line is composing one protection zone, being able to connect and disconnect according to the DCCB state, which allows the reconfiguration of the MTDC according to the events in the DC grid. The DCR connected in the output of the converter stations are  $L_1 = 600 \text{ mH}$  and the other DCR connected in the DC lines are  $150 \text{ mH}$ . The sizing of the DCR and the design of the DC breaker can be found in [3], such that the fault current is reduced, increasing the time to block of the converters blocking for the converters, therefore the DCCB time of reaction is enough to open the short circuit without blocking the MMC. In summary, the DCR value is data according to the time required to block the MMC. This way, the non-stop operation of the MTDC is assured.

In this case the DCCB has a reaction time of 3 ms to open, which is considered very fast, according to the design of a FS protection philosophy [3]. Therefore, the MTDC is composed of 8 different protection zones, 4 zones for the cables (each cable is 1 zone) and 4 zones for the stations (each station is 1 zone). The DC fault simulated occurs in the line that connects the station S1 and station S2 as done

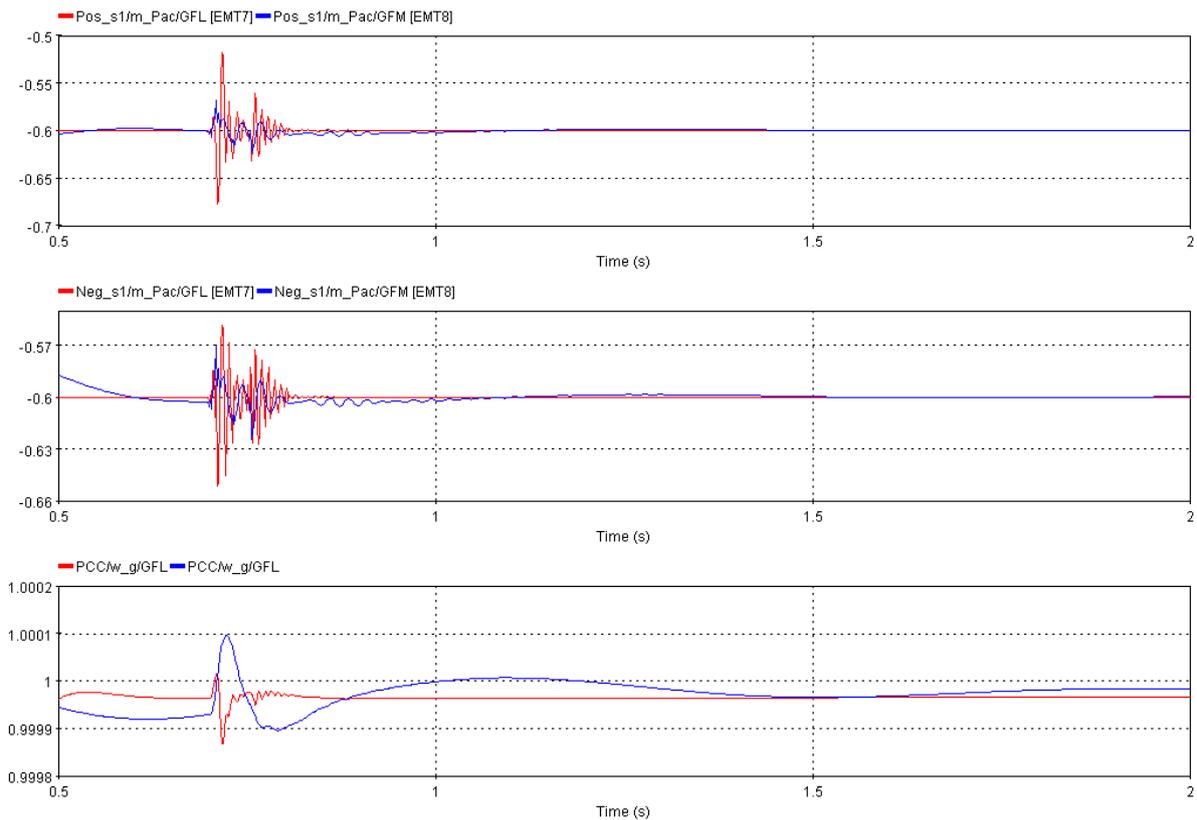
in the previous sections as a matter of comparison between the NS and the FS protection. The AC power flow is set as in Table 2-11, and the MTDC power flow is according to Table 2-12.



**FIGURE 2-82: ELECTRICAL MODEL OF THE MTDC WITH FS PROTECTION PHILOSOPHY.**

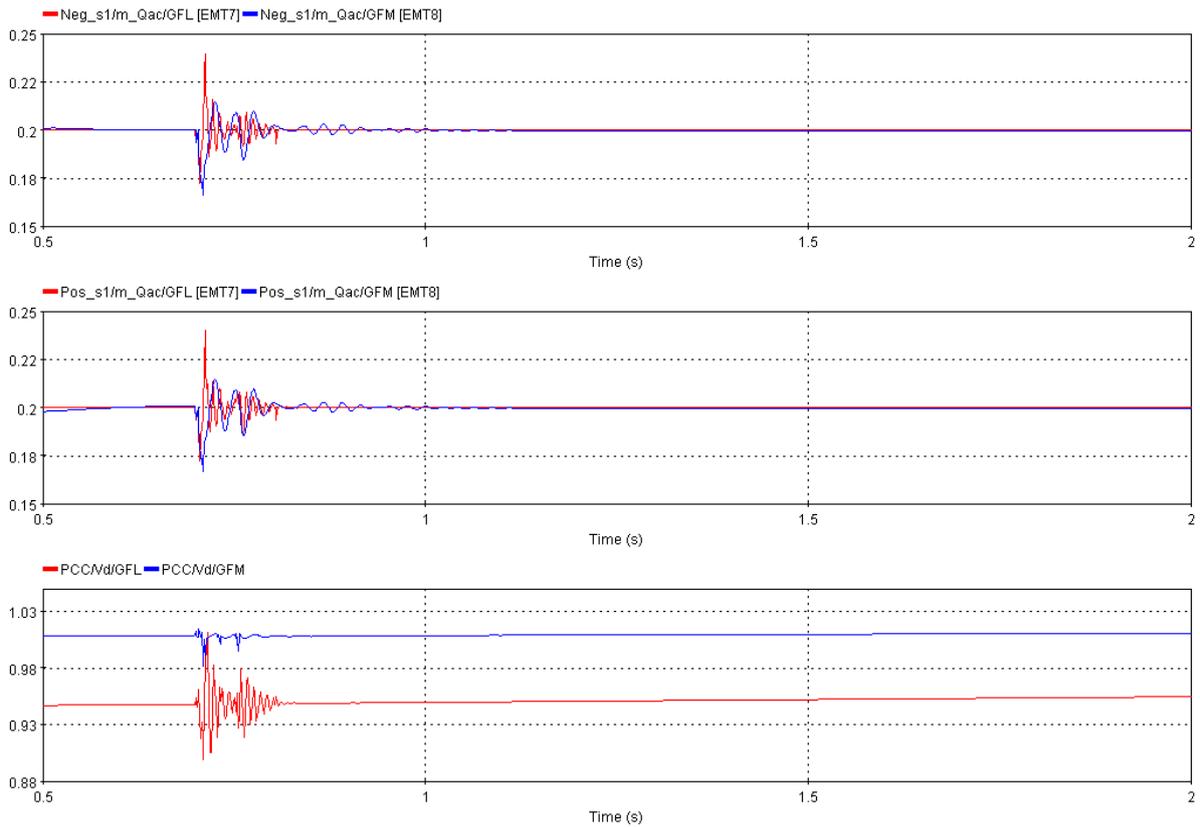
The active power profile of station S1 and the measured PLL frequency are depicted in Figure 2-83, comparing the GFL and GFM control strategies. In FS protection philosophy, the converters are not blocked, since the DCR limits the current during the fault transient, not triggering the protection of the converter, but only the DCCB that is closest to the point of the DC fault. This leads to the brief transient in both control strategies, as seen in the power profiles. The main difference is the smaller and smoother power deviations presented by the GFM control, due to the VSM response resembling a small swing of the virtual machine, since the power flow is not disturbed in this case. This is further reflected in the frequency deviation, which is as well smoother but slower, in the GFM case. Nonetheless, in both cases, the power transient caused by the disturbance is rather small and brief, not posing a concern in this DC FRT with non-stop operation of the faulty pole converter, as seen in active power and frequency profiles.

### D3.3: Protection Concepts



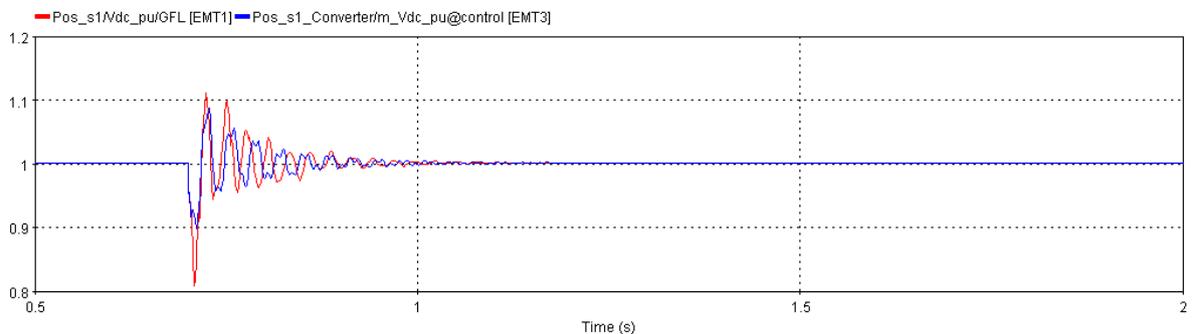
**FIGURE 2-83: ACTIVE POWER PROFILE OF STATION 1 AND THE RESPECTIVE MEASURED FREQUENCY, CONSIDERING FS PHILOSOPHY.**

Figure 2-84 illustrates the reactive power in station S1 and the AC voltage on the PCC, also comparing the GFL and GFM control strategies. Similar to the active power case, the response of the reactive power is larger and more oscillatory for the GFL control, which has no reactive power support to the AC side voltage perturbation. The voltage profile has a similar behavior during the reactive power transient, despite the fact the operating point is different for each case. As discussed in earlier subsections, GFM creates the voltage signal at its terminal, by using a droop control to share the voltage control among the converters in the bipole. Thus, even though a weak grid is connected to it, the voltage level is supported by the GFM converters, while in the GFL control strategy, the AC bus is completely responsible for voltage control in the AC grid. For both reactive power and voltage at the PCC, the fault transient during the DC FRT is not a main concern due to the speed and selectivity of the protection strategy.



**FIGURE 2-84: REACTIVE POWER PROFILE OF STATION 1 AND THE AC VOLTAGE ON THE PCC, CONSIDERING FS PHILOSOPHY.**

Lastly, the DC voltage in the positive pole (faulty pole) is presented in Figure 2-85, where the comparison between GFL and GFM control is analyzed. As mentioned above, the impact in this scenario is larger for the GFL strategy in comparison with the GFM control. Thus, DC voltage follows the same tendency, and the first drop reaches a lower minimum for the GFL control case. Nonetheless, the voltage impact is not strong enough to cause the MMC to block, therefore maintaining continuous operation of the system. In this case, the DC voltage in the GFL control is close to the limit, 0.8 pu as given in Table 2-6. But, from the DC voltage behavior, in both GFL and GFM control strategies the DC FRT with this protection strategy will not present any concern regarding the system stability.



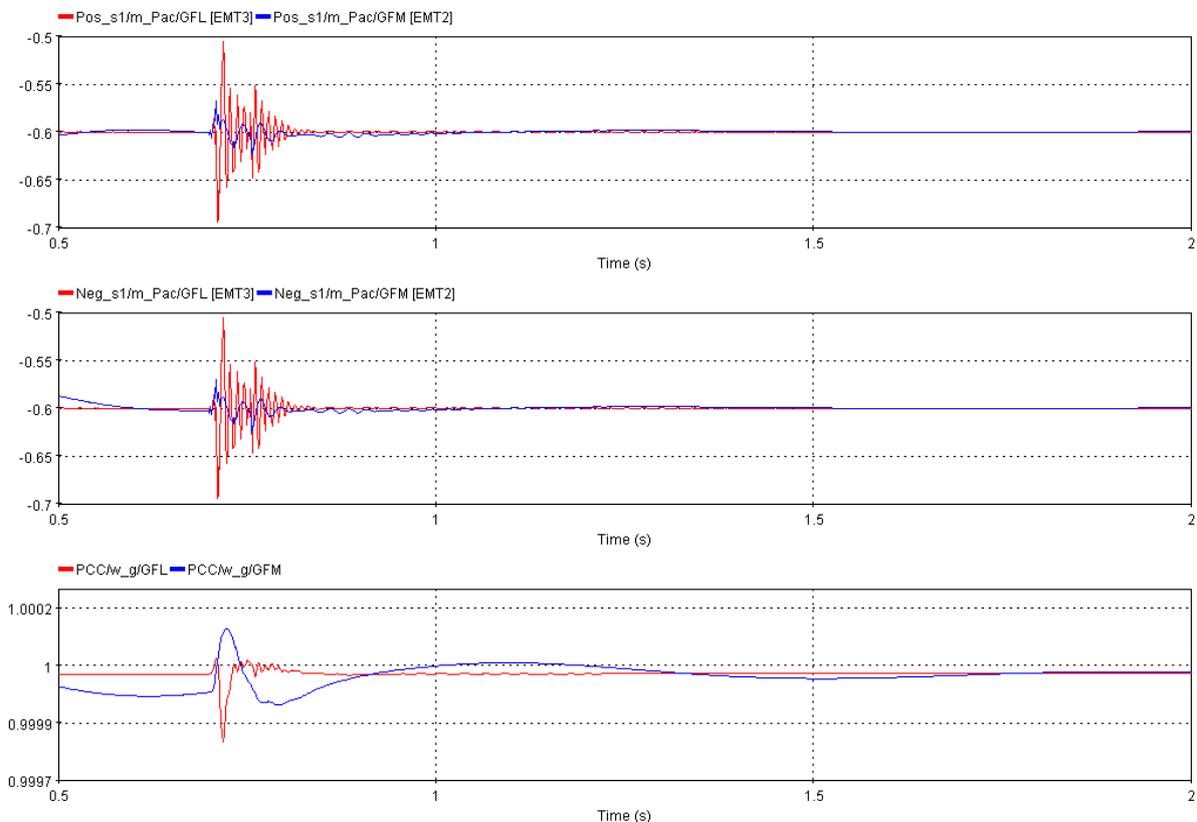
**FIGURE 2-85: DC VOLTAGE ON THE POSITIVE POLE, CONSIDERING FS PHILOSOPHY.**

### 2.5.1. Pole-to-pole fault

This subsection reviews the case of a pole-to-pole to ground fault in the fully selective protection strategy. In this case, both positive and negative poles will face a drop of voltage on the DC side, requiring a high current level to supply the fault. This can be considered a more extreme scenario, where both poles can be affected considering the protection philosophy. The fully selective strategy aims to have a non-stop operation during the DC FRT operation, being able to locate the fault and trip the DC breakers for both poles, isolating the faulty cable before the converter blocking.

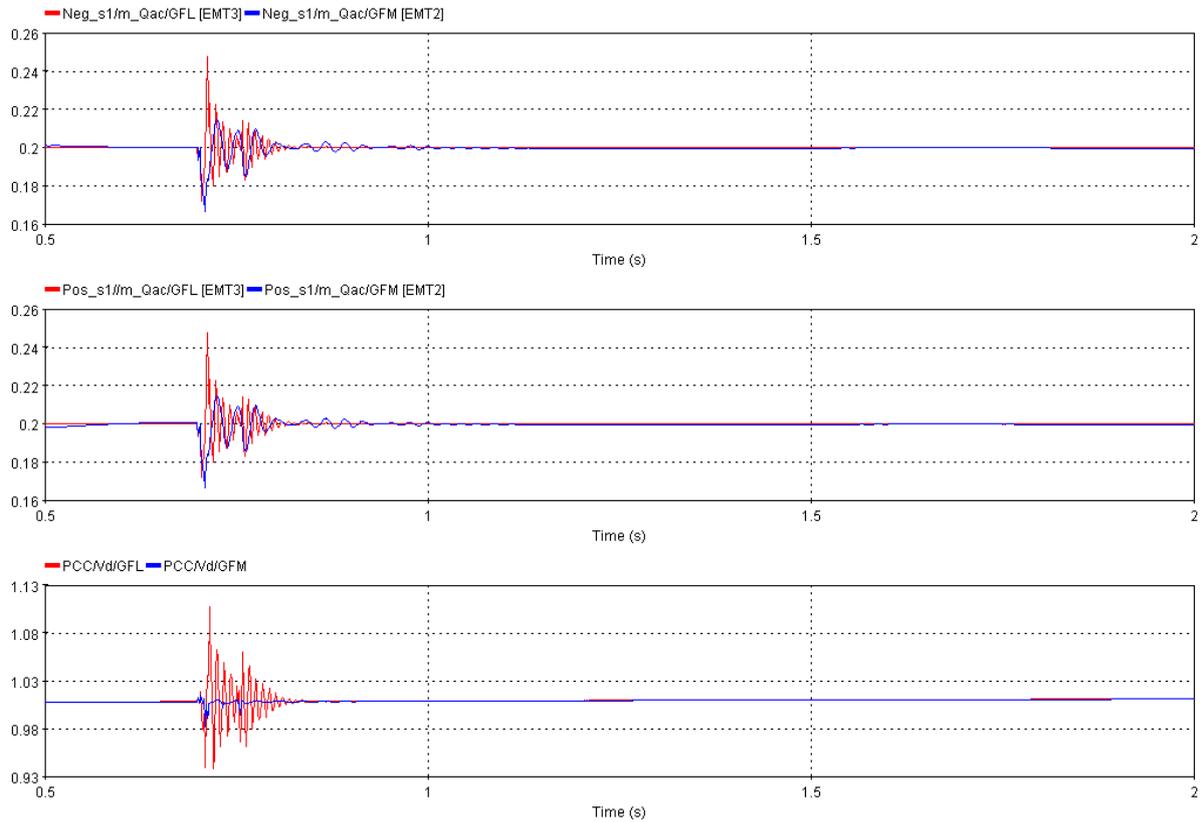
A fault is performed between the negative and positive pole to ground at the same location as the event simulated in the previous sections (cable between stations S1 and S2) with the same electrical configuration as shown in Figure 2-82.

The active power profile and PLL frequency are depicted in Figure 2-86, comparing the GFL and GFM control. The fault disturbance causes a larger reaction for the GFL control case, where stronger oscillations are encountered once the fault is cleared, since the GFL control is more sensitive to the voltage perturbations in the AC side of the grid. In the GFM case, the oscillations are smaller due to the inherent voltage source behavior of the control, both converters reduce their power output until the DCCBs opening. As of this point, the converters have a reaction to the small phase shift happening at the PCC reducing their power output. Regarding the PLL frequency, when in GFM control, it accelerates as the converters reduce the rectified power, but the perturbation is rapidly vanished, therefore, the frequency is restored with a small transient. When in GFL control the PLL frequency reacts according to the AC bus, which indicates a fast transient reduction, given by the current supply to the DC fault. But the disturbances are not big enough to cause the blocking of the affected converters.



**FIGURE 2-86: ACTIVE POWER PROFILE OF STATION 1 AND THE RESPECTIVE MEASURED FREQUENCY, IN POLE-TO-POLE FAULT.**

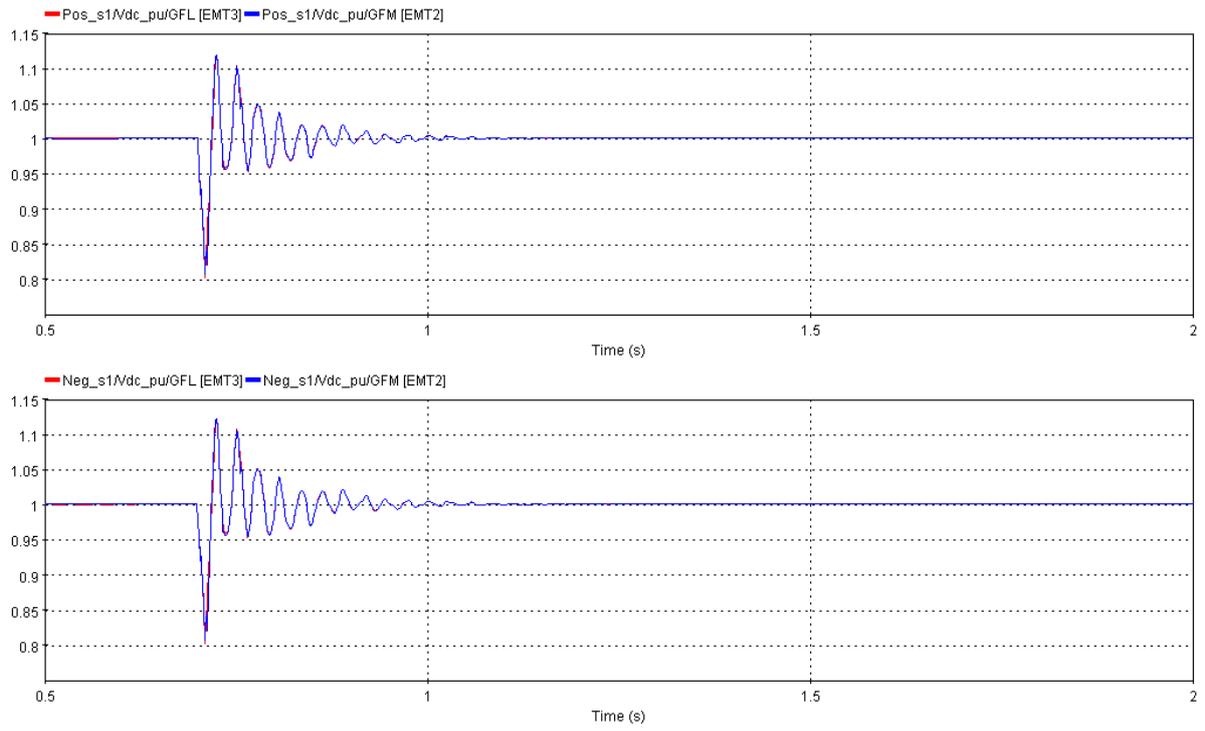
The reactive power profile in station 1 and the AC voltage on the PCC is depicted in Figure 2-87. The same tendency is seen for reactive power as in previous analysis. The GFL control strategy has a larger peak and fast oscillations that follow the short overvoltage occurring after the DCCBs open, whilst the GFM control has again a brief output reduction and softer oscillatory behavior dictated by the VSM characteristic response. The behavior of the AC voltage at the PCC is shown in the third graph of the same figure. In the GFL case, the voltage stiffness of the grid serves as the oscillation carrier for the converter output. In contrast, the GFM controls the voltage signal and maintains its level at the control objective, practically without oscillation, but only with a small drop right after the fault.



**FIGURE 2-87: REACTIVE POWER PROFILE OF STATION 1 AND THE AC VOLTAGE ON THE PCC, IN POLE-TO-POLE FAULT.**

Figure 2-88 depicts DC voltage at both positive and negative poles. In the two cases, the behavior is practically the same, as the fault location has the same relative distance to each of the converter terminals. In comparison with the pole to ground fault, the pole-to-pole fault causes a higher impact for the two control strategies tested, approaching the operational limit to non-stop operation, since the DC voltages are close to the limit ( $< 0.8$  pu the MMC blocks). But, in any case, the disturbance caused by this fault is not able impact in the system operation as resulted for the non-selective strategy.

### D3.3: Protection Concepts



**FIGURE 2-88: DC VOLTAGE ON THE STATION 1 IN POLE-TO-POLE FAULT.**

## 3. AC Protection Impacts

During AC grid faults, unaffected AC grid regions must remain in safe and stable operation and maintain continuous transmission power. To do this, it is necessary to properly detect faults and disturbances and trigger the appropriate protection equipment to quickly and safely isolate the fault. AC protection schemes are responsible for this task. Changing grid characteristics have the potential to introduce significant challenges to prevailing protection schemes as outlined in chapter 1.2. The behaviour of converters during abnormal grid conditions is primarily determined by the control structures utilised within the power electronic devices like converters. These can vary greatly depending on grid code requirements and controller design. In particular, transmission line protection schemes presently deployed in the extra-high voltage AC grids must be re-evaluated. A comprehensive and structured investigation of the effects of converter controls on the efficacy of protection relays is consequently required [35].

This study aims to provide an initial overview rather than an in-depth investigation, as those will be conducted in future work packages within EMT and HiL of this project. Therefore, this chapter presents the fundamental functions based on literature and simplified test scenarios, where distance protection is not modelled in detail, including aspects such as signal processing and filters. However, it demonstrates how fault impedance shifts when considering a weaker grid or the presence of power electronics in the network. This overview is intended to pave the way for more detailed investigations.

### 3.1. Differentiating between protection concepts

Protection, in the context of power systems, refers to the methods and technologies deployed in power systems with the purpose of detecting and handling abnormal or otherwise intolerable conditions occurring in the grid. This is achieved via the use of protective relays, which continuously monitor different aspects of the grid conditions. They typically operate either 1) proactively to prevent equipment damage – for example they may trip before an overvoltage condition leads to asset damage – or 2) reactively in response to short circuit faults and other failure conditions. Relays then interact with other devices, commonly circuit breakers, to isolate the faulty grid assets. These breakers are installed so that the detected fault can be isolated, minimising adverse effects on grid operations, energy supply, and the sensitive devices deployed in the grid [36].

There are several common types of protective methods, usually delineated by the measurements used and the algorithm used to distinguish normal and abnormal conditions. When deciding on the type of protective relay to be used in a power system, different aspects are taken into consideration, such as reliability, security, sensitivity, speed of operation, and economic factors [36]. In order to maintain a steady energy distribution, faults must be detected and cleared quickly after fault occurrence. Fault clearing time is a critical factor influencing the stability of the synchronous generators in the grid. The longest clearing time, which still maintains the synchronicity of the generators, is called the critical clearing time (CCT) [37]. In order for fault detection to be reliable, it is necessary to ensure that all credible faults are detected, with no or minimal instances of false negatives. Furthermore, it is important to avoid identifying normal grid behaviour as faults, which would result in false positives - commonly referred to as maloperations - or failure to operate during faults. Some of the different types of protection deployed in grids are [38] [39] [40]:

- **Differential protection:** This form of protection relies on a comparison of the current flowing into and out of a line. Under normal operating conditions, the sum of currents entering the line and the sum of currents exiting the line should be equal. Any deviation from this condition points towards the presence of a fault. For this process to be possible, real-time communication between relays located at both line ends is necessary typically using fibre optic links.
- **Distance protection:** This is realised via relays that monitor both the current and voltage at one end of the line and then calculate the resulting impedance. As the transmission line impedance is known, it can be used as a reference and compared against the impedance calculated from the locally-measured voltages and currents. This enables the algorithm to distinguish between faults on the protected line from faults on nearby lines. For this reason, this type of protection is also called impedance protection [39]. A challenge with distance protection is their poor selectivity in distinguishing between faults at the end of the line and faults on other transmission lines [41]. This arises due to voltage and current measurement accuracy limits and uncertainty in line impedance estimates. Distance protection can also provide time-graded backup for protection on nearby transmission lines should they fail to isolate a fault. Distance protection is often enhanced using communications-assisted protection schemes which use simple permissive tripping or trip-blocking commands. Permissive schemes typically accelerate tripping when distance protection relays at both ends of a line see the fault in the forward direction.

Distance protection is applied on almost all meshed overhead transmission lines above 100 kV. It is common for modern protection systems to be implemented using the duplicate, redundant design principle. In this approach any one component can fail, but a fully duplicate parallel path or device can still be relied upon to operate. Typically, this means two distance protection relays are used. Where suitable communications links are available, one or both relays may include differential protection as well [39]. In this project, the focus is on the distance protection relay, as it is most commonly used in HV and EHV grids.

## 3.2. Distance Protection Relay

During normal system conditions, the measured impedance will be much greater than the line impedance. When a zero-ohm short circuit fault occurs on the transmission line, the voltage at the fault location falls to zero. Thus, the impedance measured at a line end will be smaller than the line impedance. At its most basic, this is the condition that the relay uses to determine that a fault has occurred. Distance protection relays receive current and voltage signals via instrument transformers. These transformations result in the conversion of the actual impedance in the overhead line into a secondary impedance, which is smaller in magnitude but at the same angle. The combined effect of expected inaccuracies in measurements and calculations means that no protection relay of this type can monitor 100% of the line without suffering reliability issues. Therefore, a security margin of 10-15% is applied (incorrect measurement of the impedance, security margin and measurement errors). This margin avoids incorrect triggering when a fault is present near the beginning of a neighbouring line, and the relay measures a smaller impedance than is actually present. The resulting distance of the line that the relay monitors is called its under-reaching stage, also known as zone 1 [39] (see Figure 3-1).

Consequently, the line section at the end of the line would remain unprotected. For the purposes of covering this remaining part of the line, the relay is equipped with a second, over-reaching zone. The reasoning for the over-reach is two-fold: Firstly, analogously to the under-reaching stage, in the case of a fault occurring near the line end and the relay incorrectly calculating a greater impedance than

present, the relay still triggers. Secondly, the relay can provide some detection capabilities for the neighbouring line. When the scope of the implementation is widened from one relay to multiple, working in conjunction at different points in the grid, coordination between the relays is utilised to maximise their usefulness. Thus, neighbouring relays act as backups for each other in the case of one failing. This over-reaching stage, called zone 2, is always delayed, usually by up to 250-500ms. The same argument can then be used to justify additional, farther-reaching zones in both directions of the relay. Generally speaking it can be assumed, the bigger the distance covered by a zone, the larger the delay from fault detection to the triggering of breaker [38] [39]. The calculation for the load impedance is illustrated in Figure 3-1.

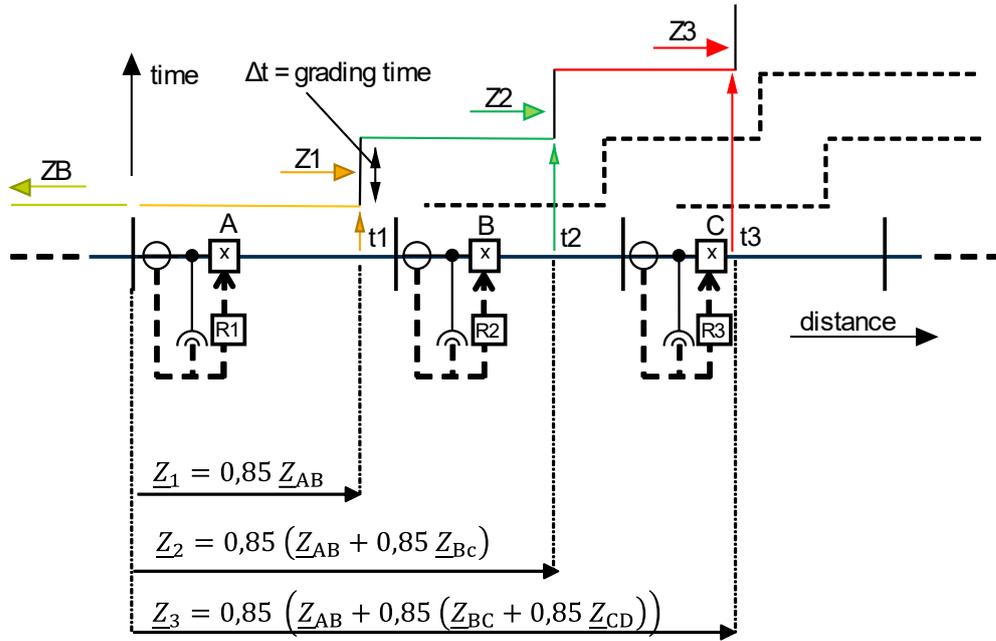


FIGURE 3-1: EXAMPLE OF GRADED DISTANCE PROTECTION ZONES.

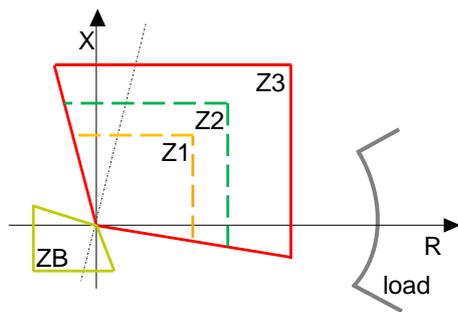
In order to comprehend the function of the individual relay, it is necessary to gain an understanding of the impedance diagram. This diagram depicts the measured impedance in the complex R-X plane. In normal operation, the relay detects an impedance corresponding to the load impedance with a value of:

$$Z_{load} = \frac{U_{line}^2}{P_{load}} \quad (3.1)$$

and an angle  $\theta_{load}$  of:

$$\theta_{load} = \text{atan}\left(\frac{P_{reactive}}{P_{active}}\right) \quad (3.2)$$

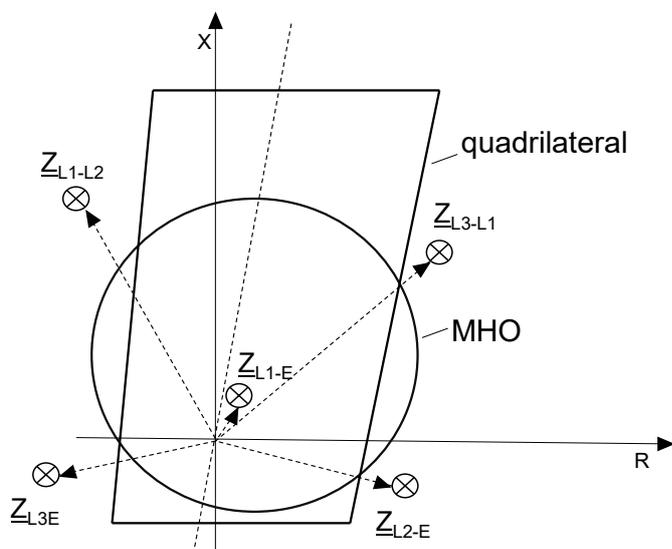
During a fault, the measured impedance will now be the short-circuit impedance, with a magnitude equal to the line impedance from the relay to the fault location and a new angle  $\theta_{sc}$ . In the case of fault/arc resistance being present, it can be taken into the consideration during these calculations [39].



**FIGURE 3-2: RELAY CHARACTERISTICS (PROTECTION ZONES- MAIN AND BACKUP)**

In Europe, quadrilateral characteristics for the impedance plane are utilised (see Figure 3-2) [42]. Distance relays can also be bidirectional, meaning that a distance relay positioned at a line end, additionally to detecting faults in front of it in the line, detect faults behind it and provide additional backup protection. When calculating the polygons utilised in quadrilateral relays, the possible fault-loop impedances are taken into consideration. In order to facilitate the appropriate handling of faults, it is necessary to have further information regarding the fault conditions. In the event of a fault occurring in the vicinity of the protection relay, this will result in the triggering of the relay's under- and over-reaching zones, as well as the over-reaching zone of the backup relay situated behind it. The aforementioned time-delays, which are associated with the further-reaching zones, are combined with permissive or blocking signals that are sent out by the relays during operation. This ensures that the relays that are situated closest to the fault act first [39]. In addition to the quadrilateral shape, the Mho shape is commonly used in the UK and North America. Unlike the quadrilateral R-X plane the Mho shape does not allow for the independent consideration of resistance (R) and reactance (X).

In the case of their failure of the main relay, the backup relays provide additional assistance in isolating the fault. Distinguishing the type of fault is also desired information for fault clearance or fault ride through (FRT) capabilities. To facilitate this, the relay calculates all impedances that may correspond to a fault, both phase-to-phase and phase-to-ground, as illustrated in Figure 3-3. An exemplary illustration, all measured fault-loop impedances during a phase to-ground fault are depicted. Only the  $Z_{L1-E}$  is detected as fault within the impedance plane, where protection relay will trip. A specifically designed tripping logic handles the incoming signals, producing a fault signal for the correct fault type [39].



**FIGURE 3-3: MEASURED FAULT-LOOP IMPEDANCES DURING A PHASE-TO-GROUND FAULT.**

### 3.2.1. Functionality

A general overview of the working principle of the protection relay is illustrated in Figure 3-4 according to the IEC 60255-121 standard [43]. The distance protection relay gets a current and a voltage signal from the bus at the beginning of the transmission line. These signals are fed into several blocks as for instance Discrete Fourier Transform that calculate the magnitudes and phases for the voltage and current signals as well as an additional current signal for the current to ground. The fundamental frequency, which serves as an input for the DFT, is set to be equal to the grid frequency.

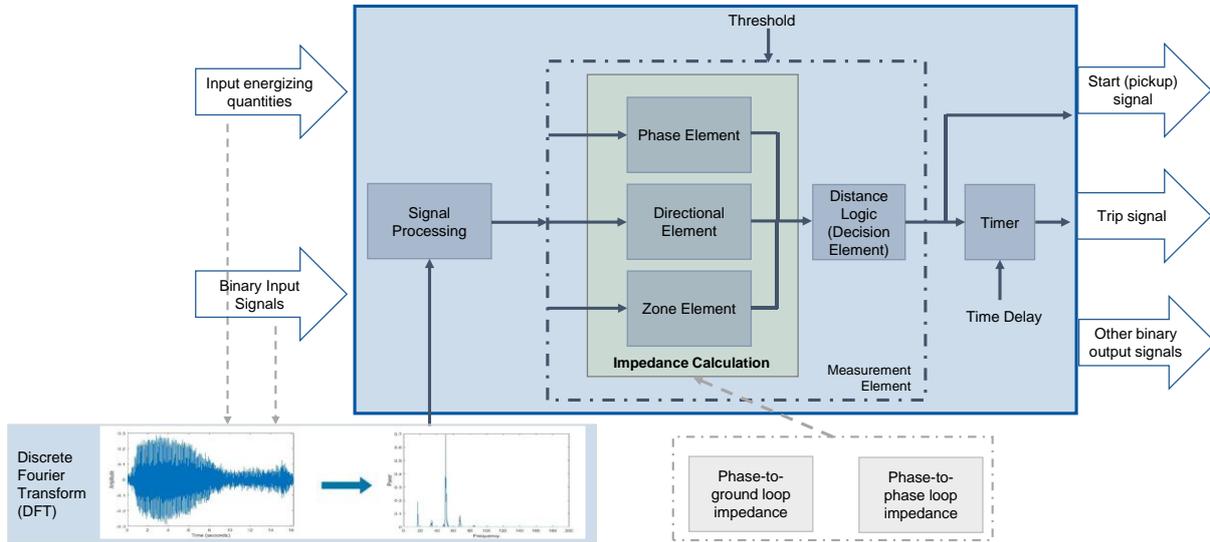


FIGURE 3-4: IEC 60255-121:2014 STANDARD FOR DISTANCE PROTECTION RELAY

These signals are then used for the following calculations to determine the impedance between phases and the impedance phase and ground:

$$\begin{cases} Z_{ph-ph} = \frac{V_{ph1} - V_{ph2}}{I_{ph1} - I_{ph2}} \\ Z_{ph-ph} = \frac{V_{ph1}}{I_{ph1} - kI_0} \end{cases} \quad (3.3)$$

The calculation of phase-to-ground loop-impedances in real world scenarios requires the addition of the factor  $k$ , which is a function of the zero and positive sequence impedances of the transmission line protected. These calculations result in  $R$  and  $X$  values for the loop-impedances.

Before being compared against the polygons representing the relay characteristics, a normalisation step is undertaken with the  $R$  and  $X$  values. These values are first transformed into polar coordinates before the magnitude component is normalised by 85% of the line impedance and 120% of the line impedance separately, so that a fault loop impedance at the edge of a protection zone ideally yields a magnitude of one for at least one scaling factor [39]. The distance protection relay model is implemented as a monodirectional relay with two protection zones, at 85% of the line and 120% of the line length. It is noted that in the literature, the additional 20% of the second zone is either taken from the original transmission line length or of the neighbouring line length, whichever is shorter [39].

The values for these normalisations are equal to the total impedance of the line on which the relay is placed. Both analytical and simulation-based approaches may be used to derive these values. Tests conducted during the modelling work showed that the difference between these two is negligible, and as such, the latter was used due to the speed with which the normalisation factor can be derived. This

procedure has practical effects, as for various boundary conditions where the line impedance may change, an explicit recalculation of the points on the R-X for the relay characteristics becomes unnecessary. Rather, the overall shape of the relay characteristics is kept constant, with only the normalisation factors being adjusted.

The phase and the scaled magnitude of the loop impedance are then transformed back into cartesian coordinates, before being compared against the relay characteristics. Due to two different normalisation factors being used for the same obtained loop impedances before any comparisons against the relay characteristics occurs, the relay is able to use the same polygon to check for faults in both zones. It is noted that different designs of the relay characteristic, specifically increases in the resistive reach, may yield different results in the occurrence of false detections. Signals for the phase-to-phase and phase-to-ground fault detections for each zone are then generated. These twelve signals (six loop impedances times two protection zones) are then fed into the switching logic in order to correctly determine the fault type and affected zone.

The switching logic handles the detection signals and seeks to determine the fault correctly. The implemented logic applies several rules, such as giving priority to fault signals for zone 1 or requiring that two phase-to-ground faults and the appropriate phase-to-phase fault signal be activated before determining a double phase-to-ground fault. For phase-to-ground faults, the presence of a minimal current-to-ground is also required. Depending on the resulting signal, appropriate triggering signals for circuit breakers are sent as outputs from the distance-protection relay block. Fault clearing has not been investigated in detail; therefore, the aspects of distance protection design are not examined here.

Within the European power grid, which is highly meshed, distance protection relays employ quadrilateral R-X characteristic for the zone element, incorporating multiple protection zones. These relays determine impedance by examining the voltage-to-current ratio. Nonetheless, shifts in the grid's characteristic can present significant challenges to existing protection relays – in particular distance protection. Variations in grid behavior have the potential to lead to relay malfunctions, including non-activation in the event of faults, which can extend the duration of voltage dips or causing response delays. Furthermore, there is a risk of over- and under-operations, with faults potentially occur outside their designated protection zones [44] [45]. Regardless of the fault, there is a chance that zone 1 fault may go undetected (under-function), while zone 2 faults could be mistakenly classified as zone 1 faults (over-function), thereby compromising the selectivity of the protection system [46]. Further grid topologies as intermediate infeed or parallel lines could affect, especially the zone 2 in the case of a fault.

The investigation are preliminary studies. Therefore, the performance with a focus on R-X detection will be tested within an IEEE 9-bus network including synchronous generators, controlled voltage sources, that are capable of imitating the behaviour of converter control concept like grid-following (GFL) and grid-forming (GFM).

### 3.2.2. Consideration of distance protection in the presence of converters

Impedance-based distance protection is a widely used method in transmission line protection, functioning on the principle that the impedance measured at the relay location can indicate a fault if it falls within predefined operational zones. By using local voltage and current measurements, the relay calculates the impedance between the fault and the relay location, ensuring that faults are detected and cleared effectively. This method has been refined over the years and remains a cornerstone of protection systems due to its simplicity and effectiveness in determining fault location and providing timely fault clearance.

However, the accuracy of impedance-based protection is influenced by several factors, including current transformer saturation, capacitive voltage transformer transients, power swings, and series compensation. These factors become even more pronounced when dealing with complex network configurations, such as resistive faults and varying control strategies. The integration of converters into the system adds another layer of complexity, as their fault characteristics differ significantly from those of traditional generation sources. Converters can cause issues like under-reach, where in-zone faults are missed, or over-reach, where faults outside the protected zone are incorrectly detected. These challenges necessitate the careful tuning and configuration of impedance-based relays to ensure reliable protection [47].

The presence of converter-based resources further complicates protection due to dynamic impedance behaviour during faults. For instance, GFL and GFM control strategies affect the positive and negative-sequence equivalent impedances of converter differently. GFL control shows more significant changes in impedance during faults compared to GFM control, particularly for phase-to-ground and phase-to-phase faults. These differences are critical for maintaining reliable distance protection, as they can lead to zone over-reach or under-reach [47] [48]. SCRs also significantly affect the equivalent impedance behaviour of converters, with lower SCRs (e.g., 2 compared to 7) causing more pronounced dynamic impedance changes, especially with GFL control. In such cases, the measured impedance locus may shift beyond the protection zone, increasing the risk of protection failure. Thus, distance protection systems must be adaptable to these variations, using advanced control strategies to ensure protection remains reliable even under varying SCR conditions [49].

During faults, particularly in resistive fault scenarios, distance protection systems can under-reach due to discrepancies in fault current from remote-end sources. This issue is prominent in meshed grids, radial connections of synchronous generators, and to a lesser extent, radial connections of converters. For radially connected converters, Zone 2 settings must be extended to account for the high impedance of transformers, though this reduces the risk of over-reaching. Maloperation due to incorrect directional determination and phase selection, as well as converter transients in the initial fault cycle, pose additional challenges that need careful configuration of the protection system [48].

Directional security can be enhanced by using zero-sequence directional elements and limiting self-polarization to instances where the memory polarization is unreliable. However, real-world applications demonstrate that sudden frequency jumps can cause zone 1 over-reach due to differences in frequency estimation between voltage and current channels. These phasor estimation errors impact the apparent impedance, requiring a more robust and adaptive approach to maintain protection integrity [48].

To conclude, the impacts discussed, along with several others, should be elaborated further in WP7. In the following sections, only some of these issues has been investigated in a generic manner. It highlights the numerous challenges associated with the increasing integration of modern technologies, such as converters and renewable energy sources, into the power grid. The complexities introduced by these elements require a deeper analysis within WP7 to ensure that protection systems can adapt and remain reliable in the evolving landscape of electrical networks.

Before enumerating different test cases, the expected interaction between converters and distance protection relay must be shortly described. In the case of a line-to-line fault, the impedance seen from the relay can be expressed as:

$$Z_{relay}^{bc} = \frac{V_{B_1}^b - V_{B_1}^c}{I_{B_1}^b - I_{B_1}^c} \quad (3.4)$$

With:

$$\begin{aligned} V_{B_1}^b - V_{B_1}^c &= kZ_l I_{B_1}^b - kZ_l I_{B_1}^c + R_f (I_{B_1}^b + I_{B_2}^b) \\ &= kZ_l (I_{B_1}^b - I_{B_1}^c) + \frac{R_f}{2} (I_{B_1}^b + I_{B_2}^b) - \frac{R_f}{2} (I_{B_1}^c + I_{B_2}^c) \end{aligned}$$

Substitution then yields:

$$Z_{relay}^{bc} = kZ_l + \frac{R_f}{2} \left( 1 + \frac{I_{B_2}^b - I_{B_2}^c}{\underbrace{I_{B_1}^b - I_{B_1}^c}_{\mu}} \right) \quad (3.5)$$

Where the factor  $\mu$  expresses the ratio of the infeed currents from the remote end of the line over the end of the line near the relay [39].

When a grid has a high penetration of SGs, this factor will tend to be of a real value, as the current infeed from SGs are similar for all SGs, given that they are predominantly determined by their physical construction. When a distance protection relay is located near a converter, the resulting characteristics of the factor  $\mu$  are heavily dependent on the control structure and may thus result in the factor  $\mu$  being imaginary. Various converters, based on the controls deployed, provide fault currents which differ both in magnitude and phase, resulting in possible impedance shifts along both the R and X axis. Thus, it is not possible to determine whether a converter will cause a resistive or reactive shift of the fault-loop impedance a-priori. As grids with lower penetrations of converters generally have higher SCR than grids with higher penetrations, this adds an additional variable when considering the factor  $\mu$ , as based on the SCR of the generation sources close to the fault, the factor  $\mu$  can vary wildly in magnitude [50] [39].

SG does not inherently generate negative sequence current, but it flows through the SG due to its low negative impedance during unbalanced faults. The negative sequence impedance of the network determines the current magnitude. In faults involving ground, the zero-sequence current creates no resultant air gap field, and the rotor windings only present leakage reactance. For fault analysis, SGs are represented by their negative sequence impedance, which is usually comparable to their positive sequence impedance. The residual impedance is the sum of the zero-sequence currents across the three phases. Fault analysis and relaying differ with increased converter penetration, as converter typically do not generate negative sequence currents unless required, as mandated by the German grid code during unbalanced faults. The negative sequence fault current from inverters depends on control, and the current magnitude is limited by the converter's VA capacity. Additionally, converters

are not expected to contribute zero-sequence current due to the lack of electromagnetic interactions, unlike SGs [51].

**TABLE 3-1: DIFFERENCES BETWEEN SGS AND CONVERTERS SHORT CIRCUITS [52]**

	SGS	CONVERTERS
<b>MAGNITUDE</b>	Up to 10~18 p.u.	1.15~1.5 p.u. (maximum)
<b>NEGATIVE CURRENT</b>	Serval time-rated current depending on negative sequence network impedance	Limited converter requirement & capacity
<b>POSITIVE SEQUENCES</b>	Yes	Yes
<b>NEGATIVE SEQUENCE</b>	Yes	No, unless designed to inject
<b>0 SEQUENCE</b>	Yes	No

Table 3-1 summarizes the short circuit of SGs compared to converters, showing that converters have a lower fault contribution, resulting in less grid damage but presenting new challenges [52]. Table 3-2 shows specific the differences between SGs, GFL and GFM behaviour.

TABLE 3-2: COMPARISON BETWEEN DIFFERENT INFEEED SOURCES.

	SYNCHRONOUS GENERATORS	GRID-FOLLOWING CONVERTER	GRID-FORMING CONVERTER
<b>GRID SYNCHRONICITY</b>	Conventional generation technology, operates synchronously with the grid frequency	Requires already existing voltage signals to be present in the grid (PLL required)	Is responsible for the forming and maintenance of grid voltage and frequency (No PLL required)
<b>OPERATION PRINCIPLE</b>	Feeds AC power into the grid	Injects current into the grid	Operates as a voltage source connected to the grid
<b>POWER CONTROL</b>	P and Q are generally coupled, represented by the power factor	Decoupled control of P and Q	Slight coupling between P and Q control
<b>APPLICABILITY IN THE GRID</b>	Established generation technology for power systems	Cannot operate at 100% penetration in the power system	Can operate at 100% penetration in the power system
<b>CONTRIBUTIONS TO GRID INERTIA</b>	Contribute to total grid inertia due to the presence of large rotating masses	Does not contribute to grid inertia	Can simulate some inertial characteristics of SGs (VSM)
<b>SCR</b>	Resistant to small disturbances, high contributions to SCR	Limited fault current, low contribution to SCR	Limited fault current, low contribution to SCR

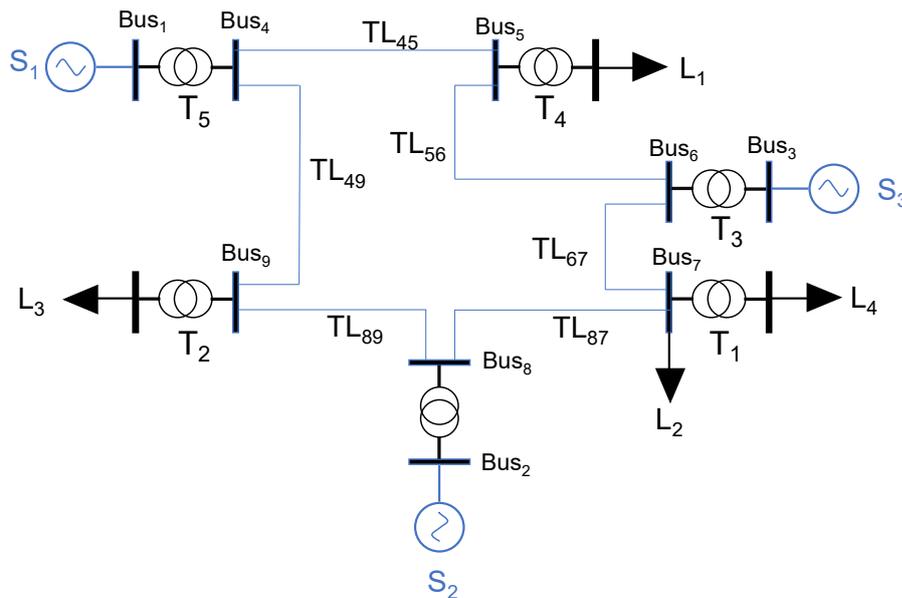
### 3.3. Investigating Protection Relay Behavior Using a Simplified Test Network

The study suggests exploring different short-circuit ratio (SCR) levels, considering the degree of synchronous generator (SG) integration versus converter prevalence. The next section presents an analysis of the IEEE 9-bus network, incorporating varying power infeed—particularly controlled voltage sources simulating GFL and GFM converter capabilities alongside synchronous generators. This model provides further indications of potential protection relay misbehaviour, warranting further investigation in work package 7.

The presented simplified test network highlights potential malfunctions in the distance protection relay, focusing on underperformance due to the R/X shift caused by varying parameters. A comprehensive parameter analysis is essential for accurate conclusions, as the current studies only provide indications of how the protection relay reacts. Future work should incorporate more complex grid configurations and examine the impact of grid topology, converter control, and line arrangements. For instance, in a parallel line scenario rather than intermediate infeed, parameter variations may lead to over-functioning, causing the relay to operate prematurely. Additionally, the AC/DC configuration, including the AC grid embedment level and DC link arrangement, should also be considered. This simplified test network highlights the importance of further in-depth investigation due to the impacts on R/X shifts.

The analysis employs a generic relay model. While future work packages may include specific manufacturers in demonstrator setups, the approach remains manufacturer-independent. Certain aspects of the signal processing model, such as filters and time constants, are simplified and may not fully represent the techniques used by all manufacturers.

The AC network model serves as the foundation of the simulation scenarios that will be analysed and it provides an extension compared to the simplified network, implementing a power flow for an AC grid at the 400-kV voltage level. The AC network model that serves as the basis for the investigation is the standardised nine-bus model provided [53]. It is comprised of three sources ( $S_1$ ,  $S_2$  and  $S_3$ ), four loads ( $L_1$ ,  $L_2$ ,  $L_3$  and  $L_4$ ), five Y-Y transformers ( $T_1$ ,  $T_2$ ,  $T_3$ ,  $T_4$  and  $T_5$ ) and six transmission lines ( $TL_{45}$ ,  $TL_{49}$ ,  $TL_{89}$ ,  $TL_{87}$ ,  $TL_{67}$  and  $TL_{56}$ ) as pictured in Figure 3-5. When simulating a system which includes a GFL, it is imperative to include at least one non-GFL source. This necessity arises from the fact that a system entirely composed of GFLs is unfeasible. At least one device in the system is responsible for a stable voltage regulation within the AC system and thereby creates the reference the GFL converters can “follow”. For a broader test setup for the investigation of the protection relay, the nine-bus network, comprising three sources, represents a suitable grid configuration.



**FIGURE 3-5: MODIFIED NINE-BUS AC NETWORK MODEL, IMPLEMENTED IN PSCAD BASED ON [53], [54].**

Several simplifications were made when modelling converters. The control structures under scrutiny (GFM and GFL) are presently implemented in various VSC technologies, the most mature of which is the MMC. As for the study only, the AC side of converters is simulated, several control loops of MMCs, such as Circulating Current Control, become obsolete. Furthermore, simplified electrical models of MMCs, consolidate the entirety of the SMs into a single capacitance per phase arm. For these MMC models, the PWM-based voltage and current control methods utilised are almost identical to those used in PWM-based VSCs [55]. It is noted here that, as more complex electrical models of the MMCs are simulated, these simplifications no longer hold, which should be considered in work package 7. In order to investigate impacts on the protection relay, a comparison between infeed sources is given below [35] [56] [37] [55] [57] [58] [59] [60]:

### 3.3.1. GFL control

The GFL component developed connects directly to the PCC in the AC grid, as would be the case with any other source component. This VSC generates voltage signals originating from the control structure directly. The basis for the control structure will be not the main focus, however, the inner and outer control loops are described below. The control structure also includes the transformation to and from the dq-reference frame of the relevant signals.

#### Inner current-control loop

The inner current control loop is depicted in Figure 3-6.

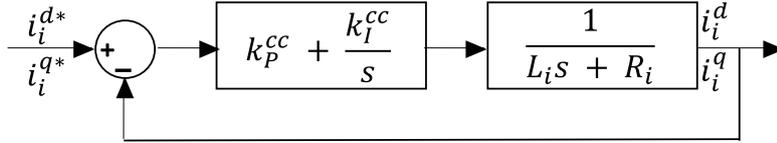


FIGURE 3-6: CURRENT CONTROL LOOP.

Through pole cancellation, the proportional and integral gains of the PI controllers are calculated as follows:

$$\begin{cases} k_p^{cc} = \frac{L_i}{\tau_i} = \omega_i L_i \\ k_I^{cc} = \frac{R_i}{\tau_i} = \omega_i R_i \end{cases} \quad (3.6)$$

Where  $\omega_i$  is the selected inner loop bandwidth,  $L_i$  is the inverter-side inductance of the LCL-filter and  $R_i$  is the inverter-side resistance of the filter [35].

#### Outer power-control loop

The outer control loop is depicted in Figure 3-7.

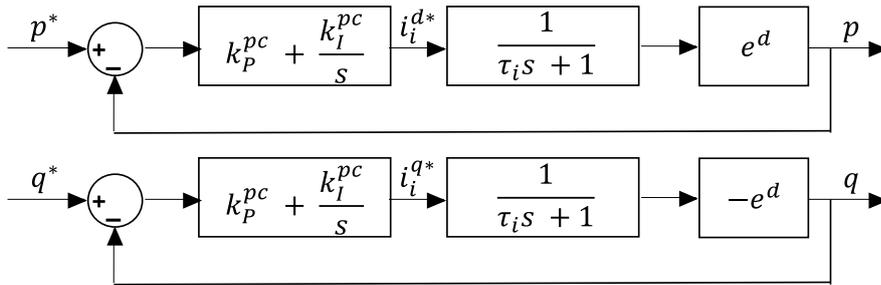


FIGURE 3-7: POWER CONTROL LOOP.

Again, using pole cancellation, analytical formulas for the control parameters are derived as follows:

$$\begin{cases} k_p^{pc} = \frac{\omega_p}{\omega_i} \\ k_I^{pc} = k_p^{pc} \omega_i \end{cases} \quad (3.7)$$

Where  $\omega_p$  represents the selected outer-loop bandwidth of the control structure [35].

### 3.3.2. GFM Control

The converter model employing the GFM control structure differs only by the presence of an outer voltage controller and a primary controller and was modelled as such.

**Primary controller**

The primary controller is modelled (Figure 3-8) and utilised a P-f droop of 1% and a Q-V droop of 2%, deployed together with limiters, capping the possible ranges of these controller outputs. In order to mitigate the effects of small transients on the stability of the GFMs, especially during the start-up process, a dead band or a PT1 controller may be used. The latter parametrized at ten-times the grid frequency was used.

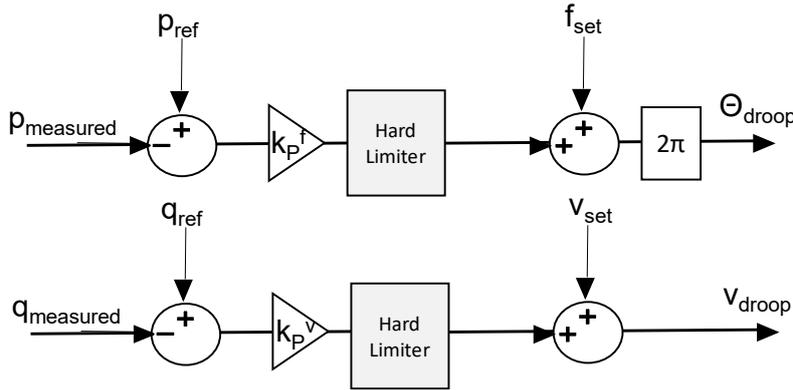


FIGURE 3-8: P-F DROOP (ABOVE) AND Q-V DROOP (BELOW) IMPLEMENTATIONS.

In general, the droop controller would provide a reference signal of  $v_{droop}$  for the d-component side of the controls, and a reference signal of zero at the q-component side:

$$\begin{cases} e_{ref}^p = v_{droop} + i_i^q L_i - i_i^d R_i \\ e_{ref}^q = -i_i^d L_i - i_i^q R_i \end{cases} \quad (3.8)$$

**Outer voltage-control loop**

The outer voltage control of the GFM was modelled with the result depicted in Figure 3-9.

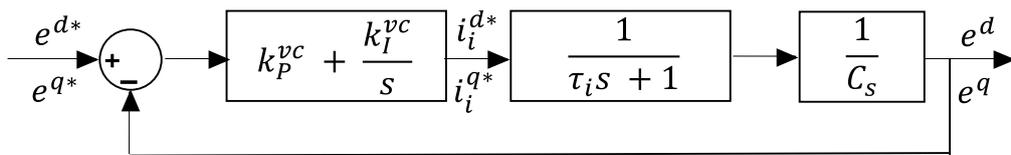


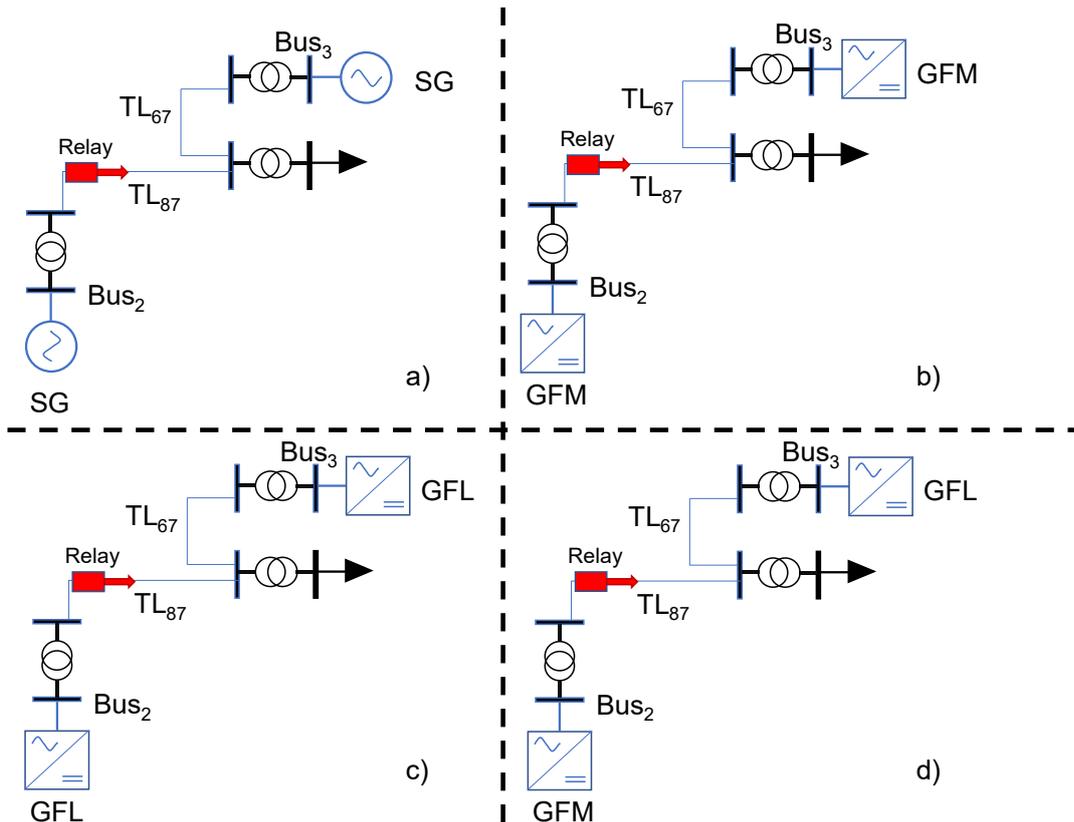
FIGURE 3-9: VOLTAGE CONTROL LOOP.

The controllers are parametrised with the method of Symmetrical Optimum, from which the following parameters for the proportional and integral gains are derived [35]:

$$\begin{cases} k_p^{vc} = C \omega_v \\ k_i^{vc} = k_p^{vc} \frac{\omega_v^2}{\omega_i} \end{cases} \quad (3.9)$$

### 3.3.3. Test Studies

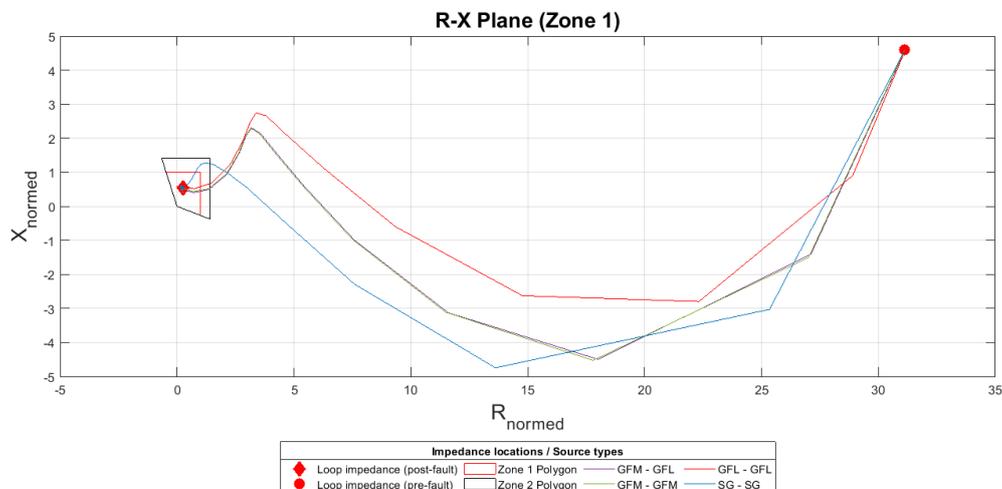
In the following Figure 3-10, each of the following scenarios have the purpose of taking one boundary condition or control parameter, varying it, and documenting the results. As there are numerous factors which may influence the fault response of converters, and thus may affect the success rate and accuracy of the distance protection relay, for each scenario only one variable will be altered, and all others will be held constant. Each of these factors represent one “degree of freedom” of what can be simulated, evaluated, and analysed. Simultaneous adjustment of multiple variables quickly causes the total number of simulation scenarios to become very large.



**FIGURE 3-10: TEST CASES CONSIDERING DIFFERENT INFED SOURCE VARIATIONS.**

The infeed sources will be connected to Buses 2 and 3, respectively. Given that the IEEE 9-node network is configured as a ring, alternative combinations for the scenarios could be considered. However, the line length between bus 2 and bus 3 is shorter. These combinations are expected to be the major factor determining the fault response of the system, and as such will be a constant point of comparison in each scenario, in order to gain a better understanding of the effects of the variables explored in each scenario. The reason for choosing is the combinations of converters are chosen, as in the presence of SGs near the fault location, the presence of a larger current infeed during the fault from the SG is expected to dominate the fault response of the system. When investigating scenarios that include a GFM converter, one possible point of variation is the primary controller present. As suggested by the prevailing literature, since these primary controllers are designed with similarly low bandwidths, no significant variations in the performance of distance protection relay, respective to different primary controllers, are observed [35]. As such, only the Droop Controller is implemented as a primary controller. These conclude the selection process of the boundary conditions of the AC grid. Subsequently, more explicit adjustments in the control parameters of the converter combination will

be addressed. Firstly, the bandwidths of the converters are varied, followed by variations of the allowed overcurrent. The former is directly relevant to the control parameters of converters, whereas the latter is relevant due to the presence of the current reference-saturation limiter.



**FIGURE 3-11: MOVEMENT OF A MEASURED LOOP-IMPEDANCE FROM PRE-FAULT TO POST-FAULT CONDITIONS (86KM)**

Furthermore, unless stated otherwise, the loop-impedances depicted are measured phase-to-phase. Any R- plane denoted as “one” depicts the impedance plane after being scaled with the value used to test for faults in the first impedance zone. This means that the impedance measurements are scaled by 85% of the line impedance. As such the axis of the R-X planes here are dimensionless. The scaling factors used are presented whenever relevant.

All faults induced have an impedance of 1,35  $\Omega$  and are three-phase-to-ground faults located at the middle of the line unless stated otherwise. It is important to consider that all relevant loop impedances are constantly being measured by the relay. This means that the measured impedances, when observed in the R-X plane, move from a point removed from the relay characteristic during normal operation, to within it or near it after a fault, within a fraction of a second. An illustration of this, specifically for a three phase-to-ground fault in the middle of the line (TL<sub>87</sub>), is pictured in Figure 3-11. Further, the distance between the two infeed sources has been varied to investigate at the same time the electrical closeness of the controlled sources and to identify different influencing factors of the control concept.

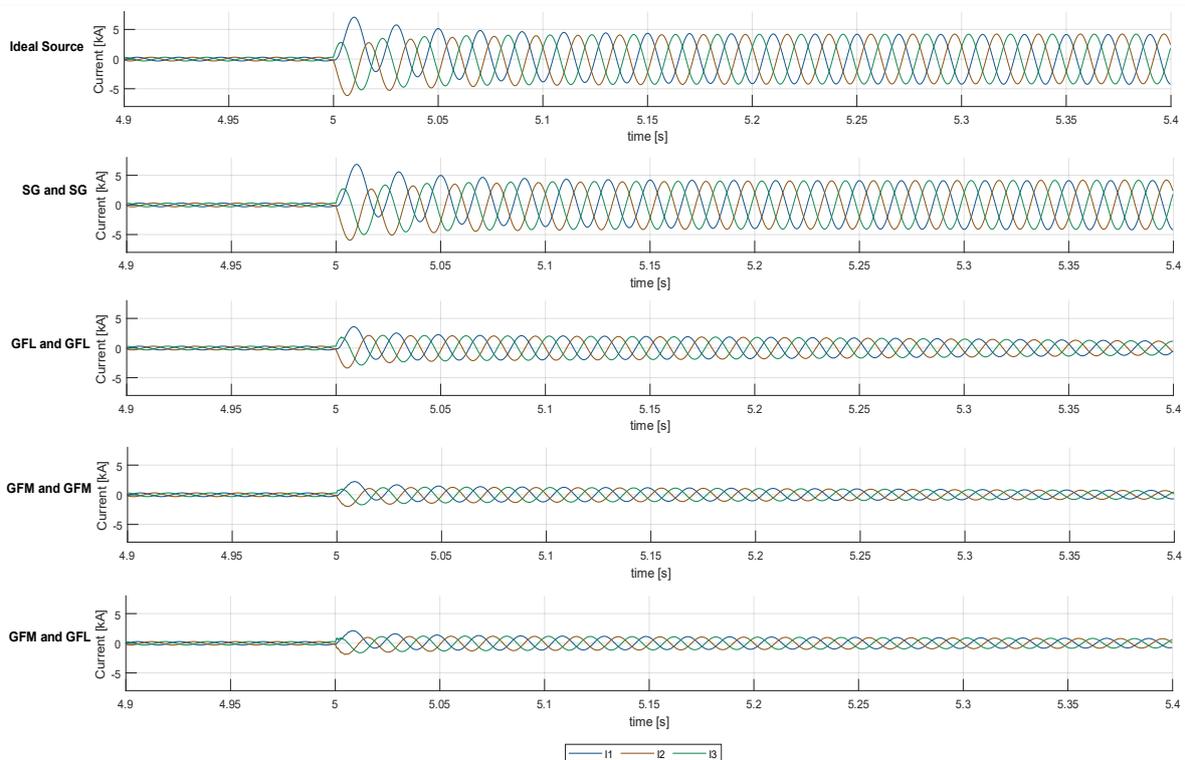
The scenarios pertaining to this group are as follows:

- **Varying the control-loop bandwidths:** As the desired control-loop bandwidths can be chosen during the parametrisation of the converter control structures, the effects of this design decision on the performance of distance protection in the resulting grids will be explored. For each scenario, the ratio of the bandwidths (signal processing) between the inner and outer control-loops, for GFMs and GFLs, will be held to a constant ratio.
  1. Symmetric variations in the control-loop bandwidths, where the bandwidths for GFMs and GFLs are increased or decreased by the same ratios.
  2. Asymmetric variations in the control-loop bandwidths, where the bandwidths for the GFM and GFL are adjusted by different amounts.

- **Varying the current-limitation methods:** The two prevailing methods of current-limitation in converters, current reference saturation and virtual impedance limitation, and their effect on distance protection will be explored. Furthermore, possible design decision in the converter control parametrisation, such as the allowed maximum current infeed, will also be explored. As was the case for the previous scenario, both symmetric and asymmetric adjustments for these parameters is possible.

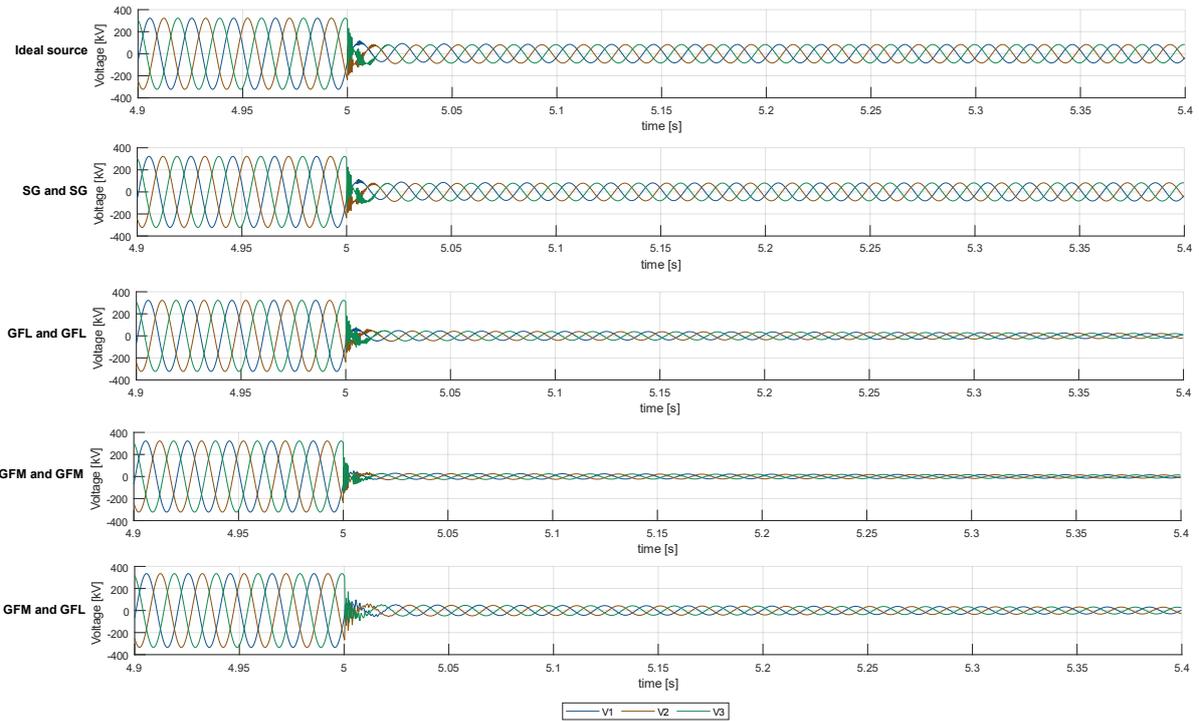
In the preliminary studies, only a three-phase-to-ground fault with a fixed fault impedance of 1,35 Ohm has been considered. This approach was chosen as the converter models are fully capable of handling these types of faults. Simulating only this fault type ensures a better comparison when examining the influence of specific control parameters. It is also noted that, for faults such as phase-to-phase faults, higher fault impedances than those simulated could occur, leading to a greater shift in the measured impedance. For each line length, three-phase-to-ground faults at 50% of the line length are simulated. This specific location is chosen to analyse faults near the first impedance zone limit of the protection relay and near the line end. The geometry of the overhead transmission line and the conductor type (264-AL1/34-ST1A) provide important details for calculating the line's capacitance and inductance. As a base case for the model, a current loop bandwidth of 2kHz was used, whereas the voltage controller has a bandwidth of 200 Hz and the power controller has a bandwidth of 3 Hz.

Starting from the initial point (middle of the 86 km line), the following current and voltage curves can be observed. In this case, the fault was applied at 5 seconds; however, in later investigations, the fault was applied at 10 seconds.



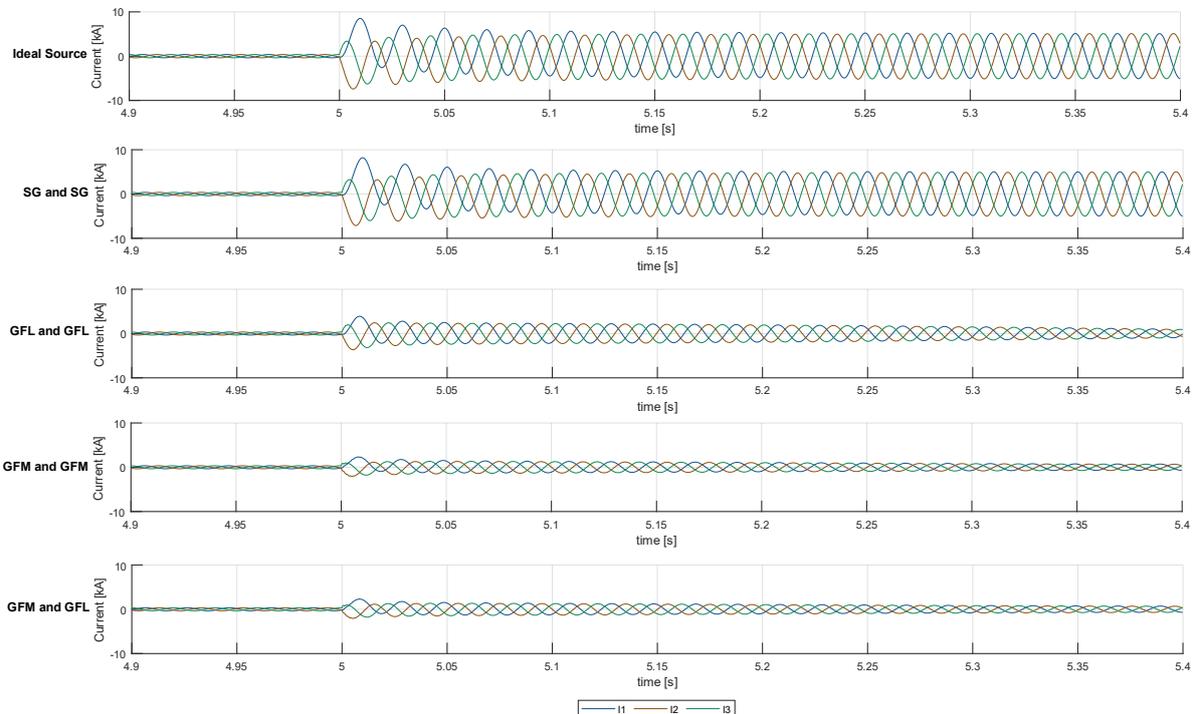
**FIGURE 12: CURRENT CURVES FOR VARIOUS COMBINATIONS: IDEAL SOURCE, SG AND SG, GFL AND GFL, GFM AND GFM, GFM AND GFL (86KM)**

### D3.3: Protection Concepts



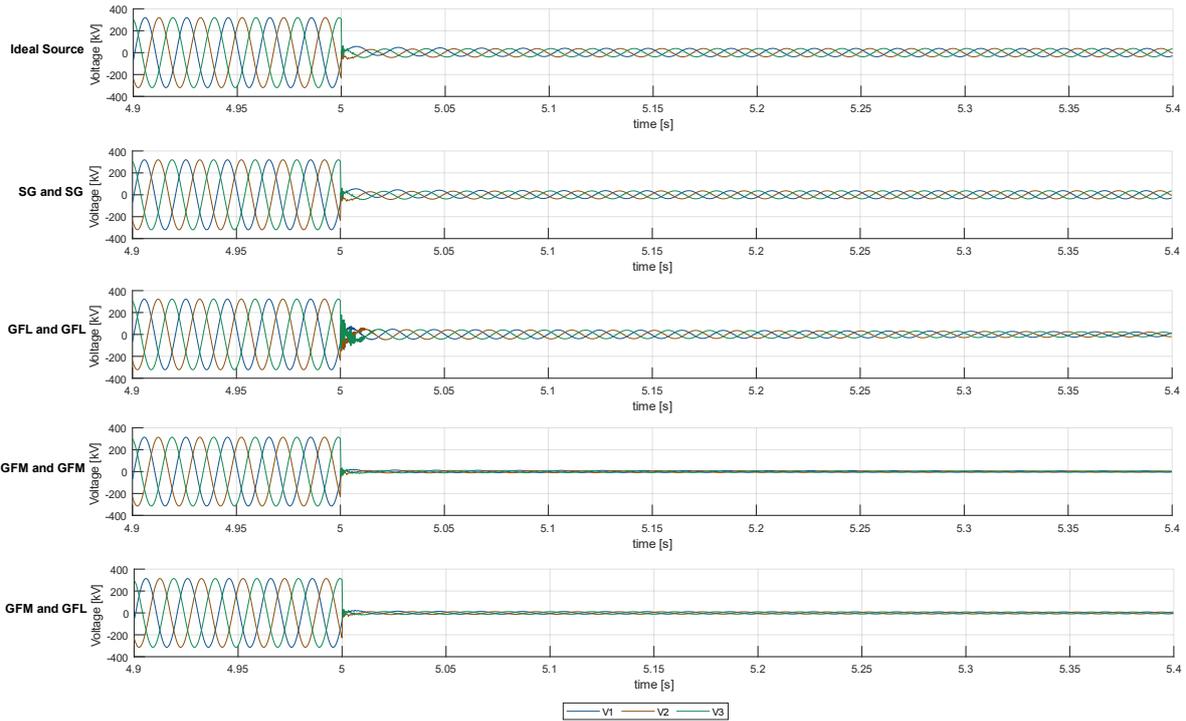
**FIGURE 13: VOLTAGE CURVES FOR VARIOUS COMBINATIONS: IDEAL SOURCE, SG AND SG, GFL AND GFL, GFM AND GFM, GFM AND GFL (86KM)**

When  $TL_{87}$  is reduced to 20 km, the following curves are generated from the simulation:



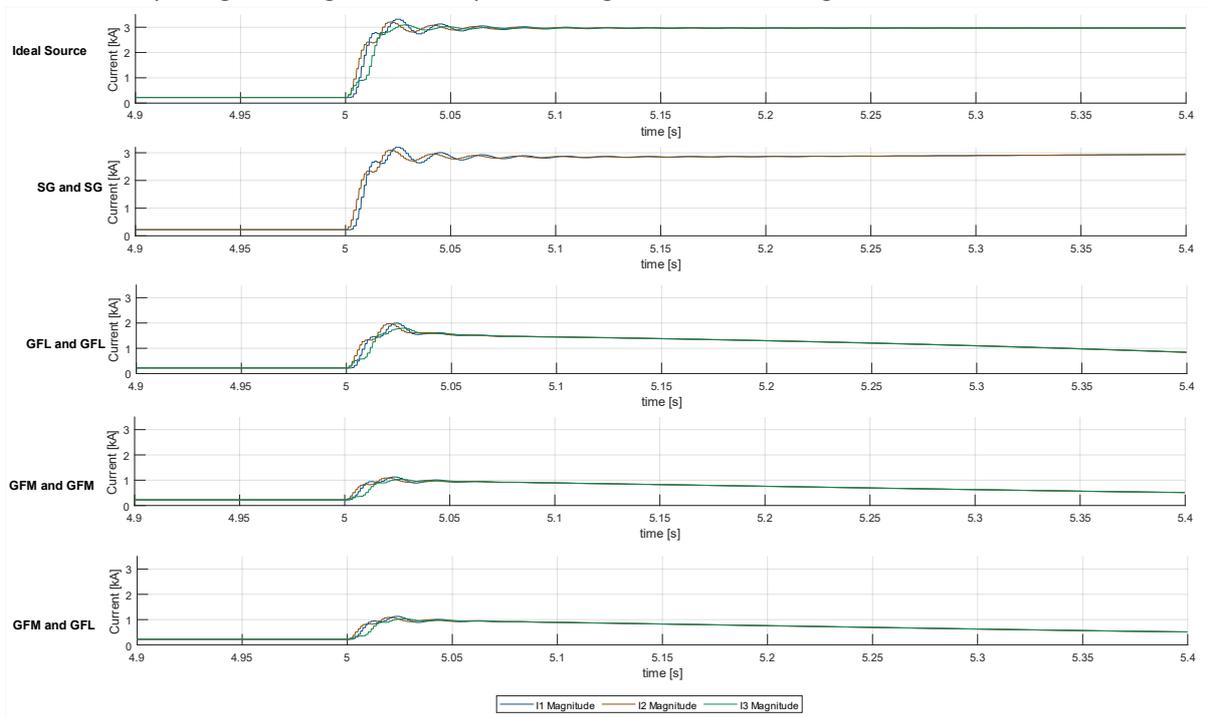
**FIGURE 14: CURRENT CURVES FOR VARIOUS COMBINATIONS: IDEAL SOURCE, SG AND SG, GFL AND GFL, GFM AND GFM, GFM AND GFL (20KM)**

### D3.3: Protection Concepts



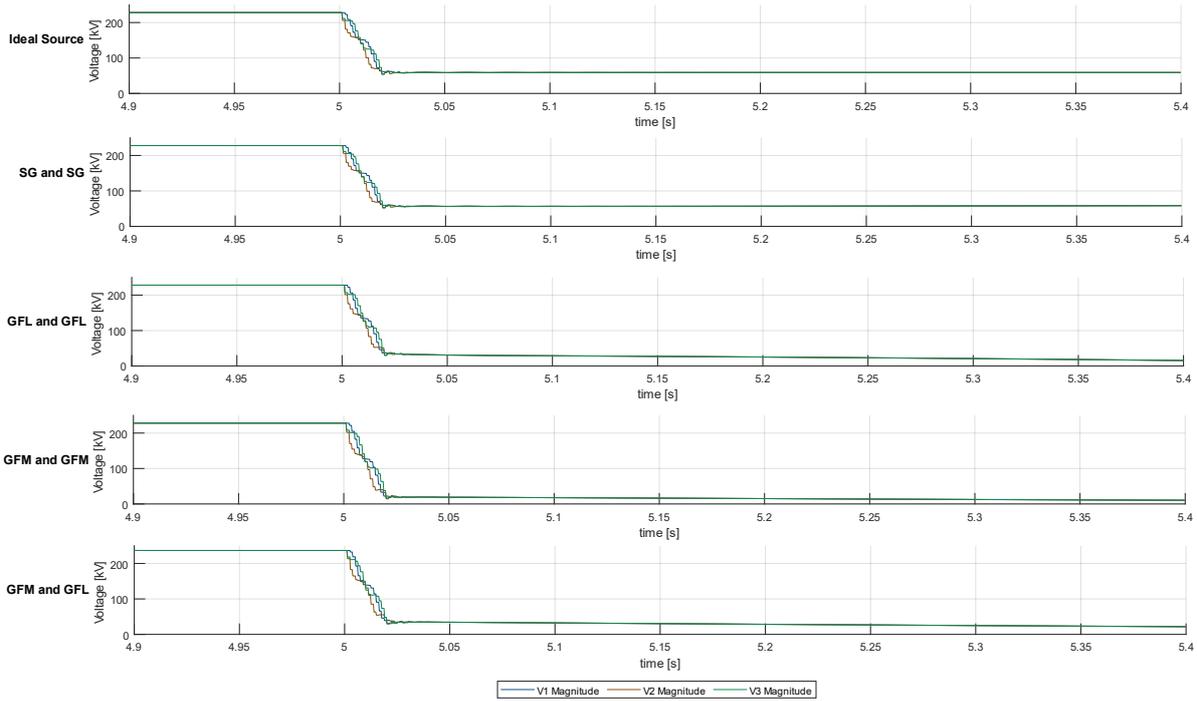
**FIGURE 15: VOLTAGE CURVES FOR VARIOUS COMBINATIONS: IDEAL SOURCE, SG AND SG, GFL AND GFL, GFM AND GFM, GFM AND GFL (20KM)**

After decomposing the magnitude and phase using FFT, the following curves were simulated:



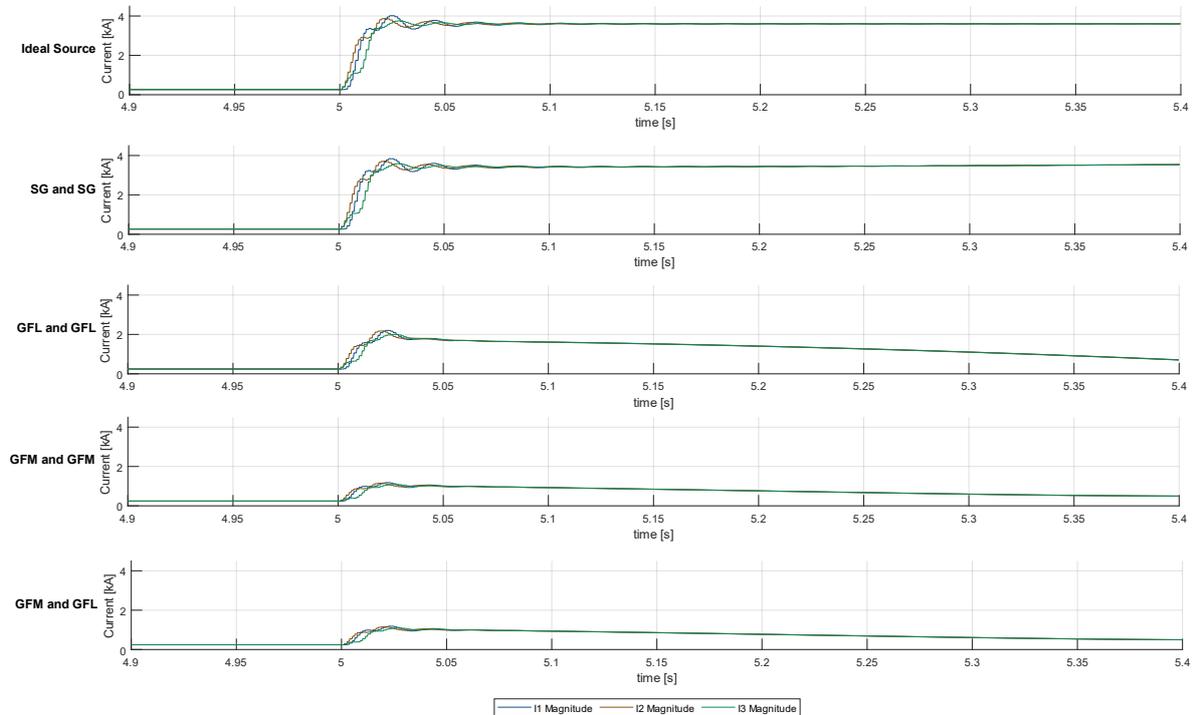
**FIGURE 16: CURRENT MAGNITUDES AFTER THE FFT FOR VARIOUS COMBINATIONS: IDEAL SOURCE, SG AND SG, GFL AND GFL, GFM AND GFM, GFM AND GFL (86KM)**

### D3.3: Protection Concepts



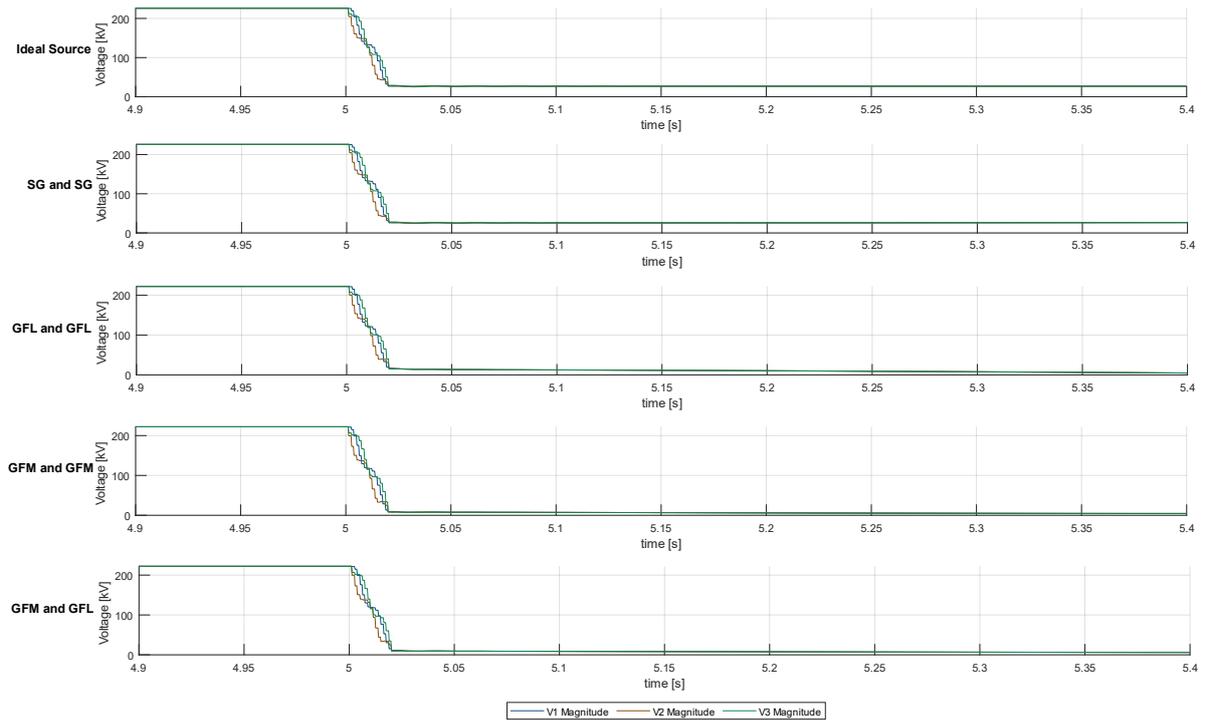
**FIGURE 17: VOLTAGE MAGNITUDES AFTER THE FFT FOR VARIOUS COMBINATIONS: IDEAL SOURCE, SG AND SG, GFL AND GFL, GFM AND GFM, GFM AND GFL (86KM)**

Again, when  $TL_{87}$  is reduced to 20 km, the following magnitudes for current voltage are generated from the simulation:



**FIGURE 18: CURRENT MAGNITUDES AFTER THE FFT FOR VARIOUS COMBINATIONS: IDEAL SOURCE, SG AND SG, GFL AND GFL, GFM AND GFM, GFM AND GFL (20KM)**

### D3.3: Protection Concepts

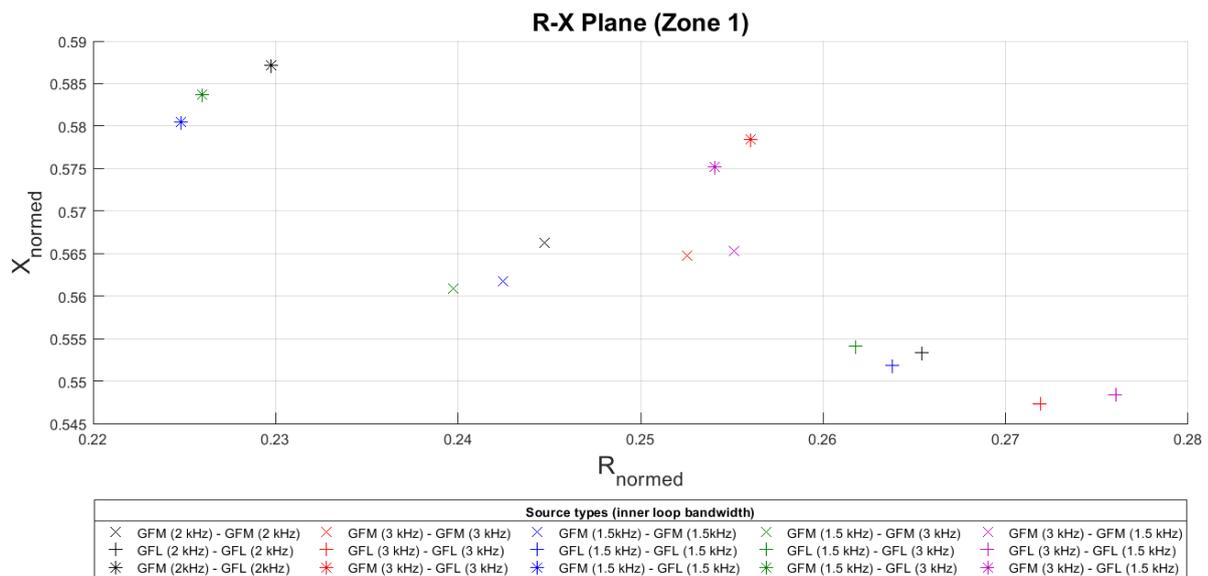


**FIGURE 19: VOLTAGE MAGNITUDES AFTER THE FFT FOR VARIOUS COMBINATIONS: IDEAL SOURCE, SG AND SG, GFL AND GFL, GFM AND GFM, GFM AND GFL (20KM)**

### Variation of the control-loop bandwidths (inner loop)

When adjusting the control-loop bandwidths, both the inner- and outer-loop bandwidths are adjusted in identical manners. Asymmetrical adjustments of these two parameters can easily cause instabilities in the model, as was often witnessed during the modelling process. A consequence of these adjustments is often undesirable changes in the phase-margins available. Thus, when presenting the different situations simulated, only the inner-loop bandwidth will be documented, as the outer-loop bandwidths will be similarly adjusted. For the following simulations, bandwidths of 2 kHz (start point), 3 kHz and 1.5 kHz are used. The other two bandwidth configurations 1,5 and 3 kHz seek to evaluate the effect of lowering or raising the bandwidth on the fault behaviour. Furthermore, asymmetrical parametrisations between the two converters are simulated. Results obtained from faulting the 86 km and the 20 km line configuration (TL<sub>87</sub>), are shown in Figure 3-20 and Figure 3-21. A three-phase fault to ground with a fault resistance of 1.35 Ohm was applied. Comparing with the start point of 2 kHz Figure 3-20 the normalized impedance with an ideal source for the 86 km line is  $R_{normed,86} = 0,2405$  and  $X_{normed,86} = 0,5727$ . For the 20 km line (Figure 3-21), he normalized impedance with ideal sources is  $R_{normed,20} = 0,08475$  and  $X_{normed,20} = 0,5833$ .

Specifically, adjustments to the bandwidth of the PI controllers are highlighted as a potential problem source, as even though the changed transients they introduced disappear after less than 100 ms in the concrete case, it is precisely this time-range that is critical for the protection of AC grids.



**FIGURE 3-20: VARIATIONS IN THE CONTROLLER BANDWIDTH (86 KM LINE)**

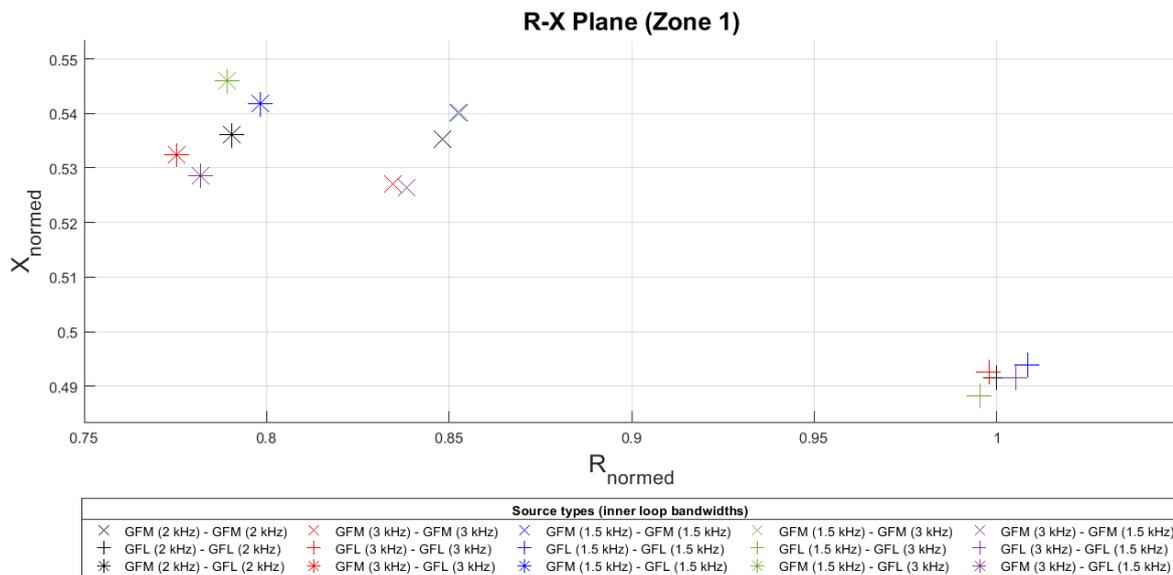


FIGURE 3-21: VARIATIONS IN THE CONTROLLER BANDWIDTH (20 KM LINE)

Generally, in both models with the different line lengths, similar trends are observed. The influence of the bandwidth on the fault-loop impedance is minor. Furthermore, the bandwidth of the converter closer to the fault is observed to be the dominant factor. When, for example, examining the configurations with two GFMs in the model utilising the 20 km long lines, the outcomes observed are dictated by the bandwidth of the converter closer to the fault. In the case of this converter having an inner-loop bandwidth of 1.5 kHz, the two fault-loop impedances are near identical even when the bandwidth of the GFM connected to bus three is changed. To better understand what is happening, the transient behaviour of the system must be examined in further detail. It is noted that the primary controller of the GFMs were not adjusted, meaning that in each case the reference signals fed into the control structure should be same. The same is true for GFLs, who have predetermined P and Q reference signals. This implies that the differences observed are also a transient behaviour. In Figure 3-22, the measured resistive impedance from the protection relay for the phase-to-phase fault, just after it occurs at  $t = 10$  s, is depicted. Specifically, the configurations with two GFMs are presented.

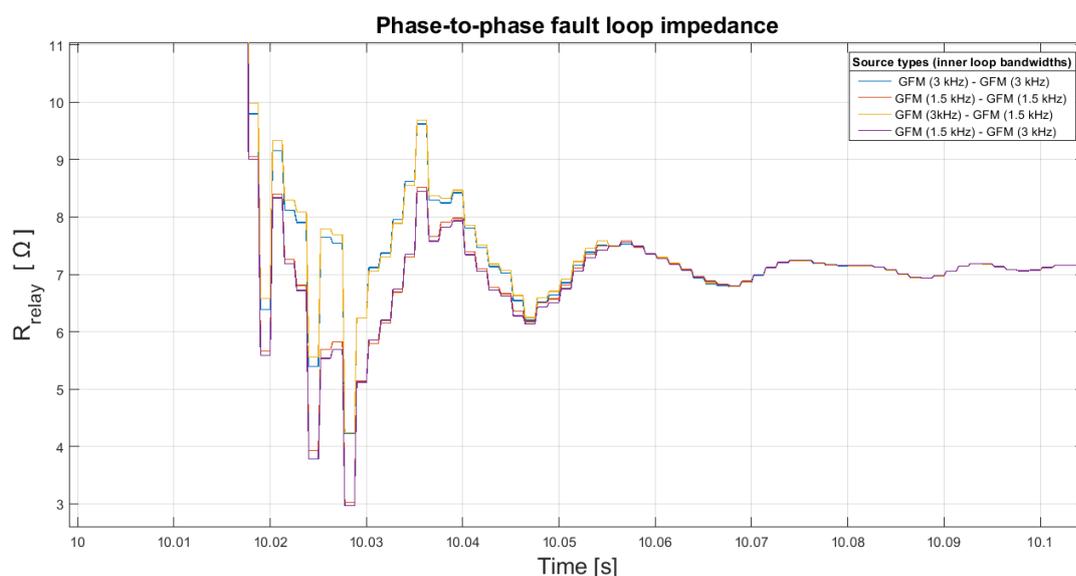
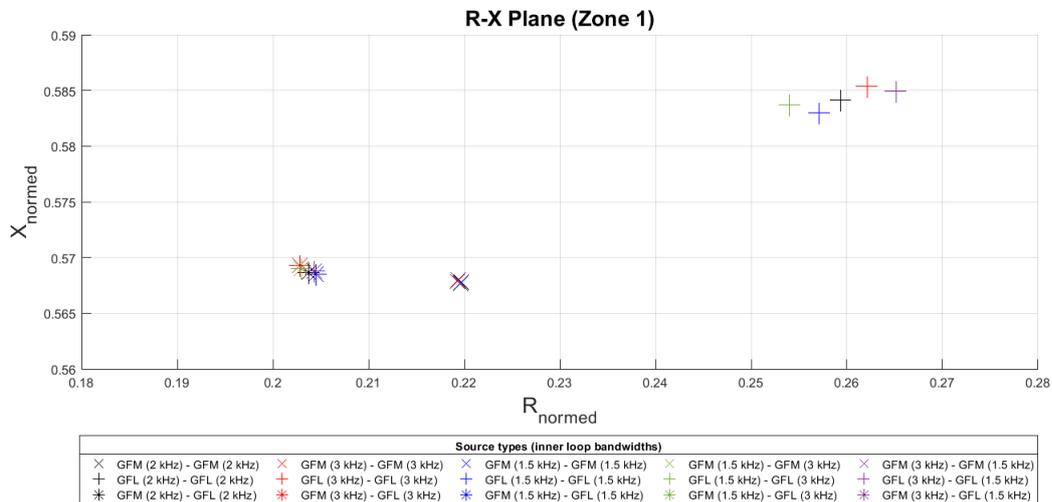


FIGURE 3-22: FAULT-LOOP RESISTANCE BETWEEN TWO GFMS.

It is observed from the figure that in approximately the first 50 ms after the fault occurs, there are deviations between the transient impedances measured. Again, the transients seem to be determined by the bandwidth of the GFM located closer to the fault location. The overshoot during this transient also correlates with this bandwidth. However, after this initial transient, the measured impedances converge. The results for the 86 km model, sampled 40 ms later at  $t = 79$  ms, as depicted in Figure 3-23, paints a similar picture.



**FIGURE 3-23: VARIATIONS IN THE CONTROLLER BANDWIDTH (86 KM LINE).**

Here, for the configurations with two GFMs, GFM-GFL combination, the measured impedances have converged significantly. The impedances for the configurations with two GFLs have also converged to a lesser extent. The absence of a primary controller in the system causes the oscillations resulting from the saturation of the converter currents to diverge slightly. Since in these configurations the source providing the reference voltage for the GFLs is located at bus one of the models, and thus further away from the fault than either converter, these results are to be expected.

In summary, the bandwidth of the converter near the fault, affects the transient immediately post-fault, and therefore also affect the measured fault-loop impedance. As these first tens of ms are relevant to protection mechanisms, the effect of controller bandwidths has an impact on the performance of the protection relay.

### Variation of the current-limitation methods

In this section, the impact of the maximum allowed converter-current on the viability of distance protection relays is studied. In the simulations up to this point, a current reference saturation limiter has limited the current feed-in of the converters to 1.3-times (1.3 p.u.) the operating current. In the following simulations, for models with 86 km lines and 20 km lines, variations in this value are simulated. Firstly, both of the converters have their maximum allowed currents limited to 1.15 p.u. Following this, asymmetrical adjustments between the two converters are simulated, where one is limited to 1.15 p.u. and the other to 1.3 p.u. Comparing with the start point again (2kHz, three-phase to ground with a fault resistance of 1.35 Ohm in the middle of  $(TL_{87})$ , For the 86 km line (Figure 3-24) the normalized impedance with an ideal source is  $R_{normed,86} = 0,2405$  and  $X_{normed,86} = 0,5727$ . For the 20 km line (Figure 3-25), he normalized impedance with ideal sources is  $R_{normed,20} = 0,08475$  and  $X_{normed,20} = 0,5833$ .

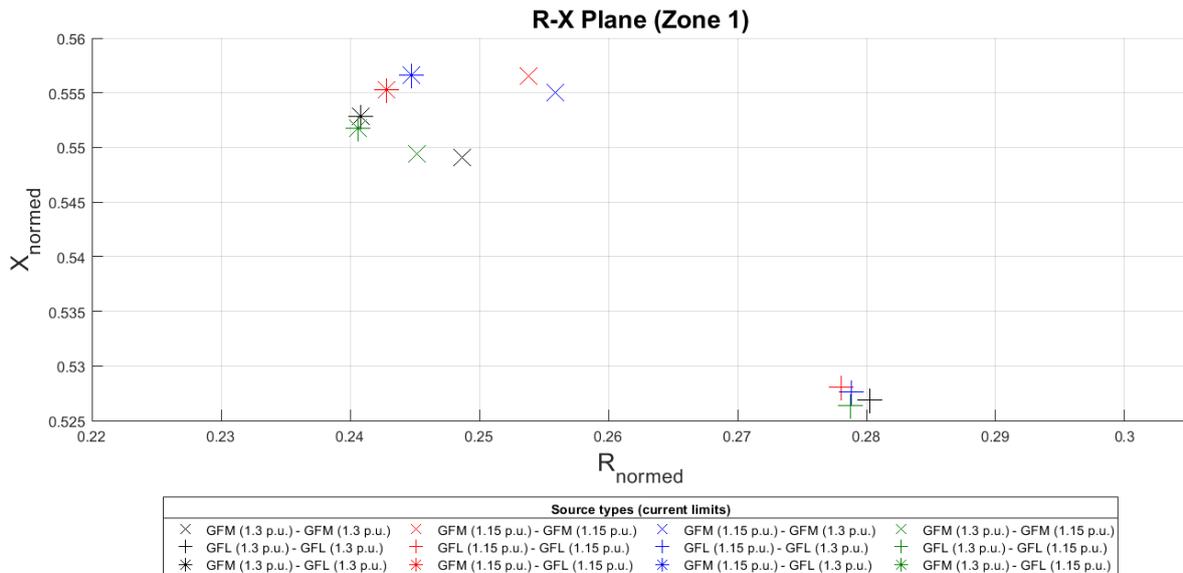


FIGURE 3-24: VARIATIONS IN THE CURRENT LIMITS (86 KM LINE).

Evaluating results for the 86 km line model, similar trends to the previous section are initially observed. Specifically, it seems that the current limit of the converter located near the fault determines the slight variances in the measured fault-loop impedance. However, the results from the 20 km line model as depicted in Figure 3-25, introduce some differences.

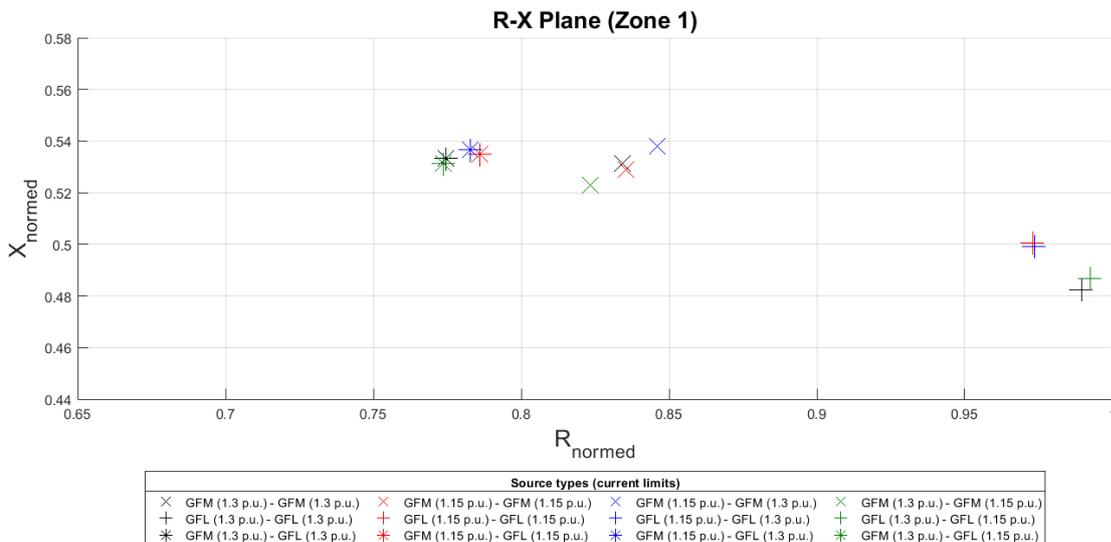
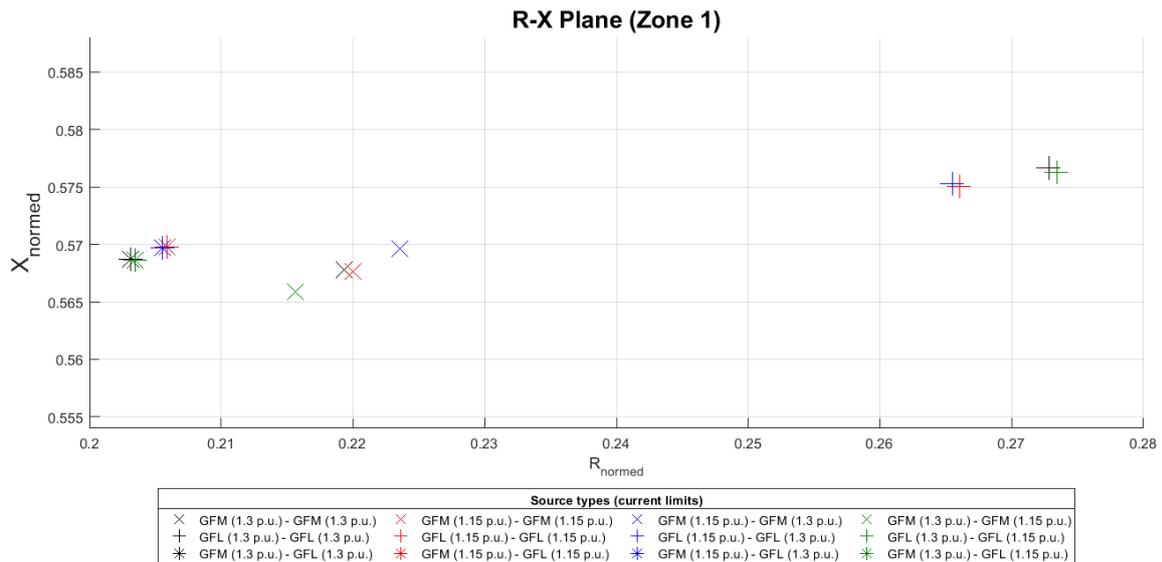
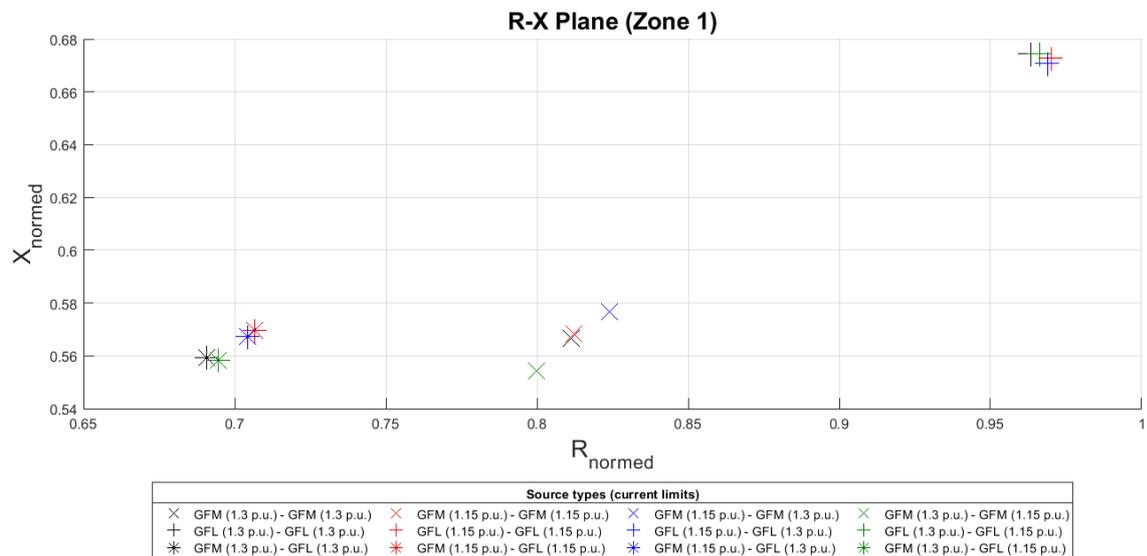


FIGURE 3-25: VARIATIONS OF THE CURRENT LIMITS (20 KM LINE).

For the two GFL and the GFM/GFL configurations, similar results to Figure 3-24 are observed. On the other hand, for the configurations with two GFMs, the impedances for the simulations where the two converters had the same current limit (per unit) have converged. In order to gain a better understanding of these results, the relevant fault-loop impedances are again sampled at  $t = 79$  ms after the fault occurrence, as depicted in Figure 3-26 and Figure 3-27.



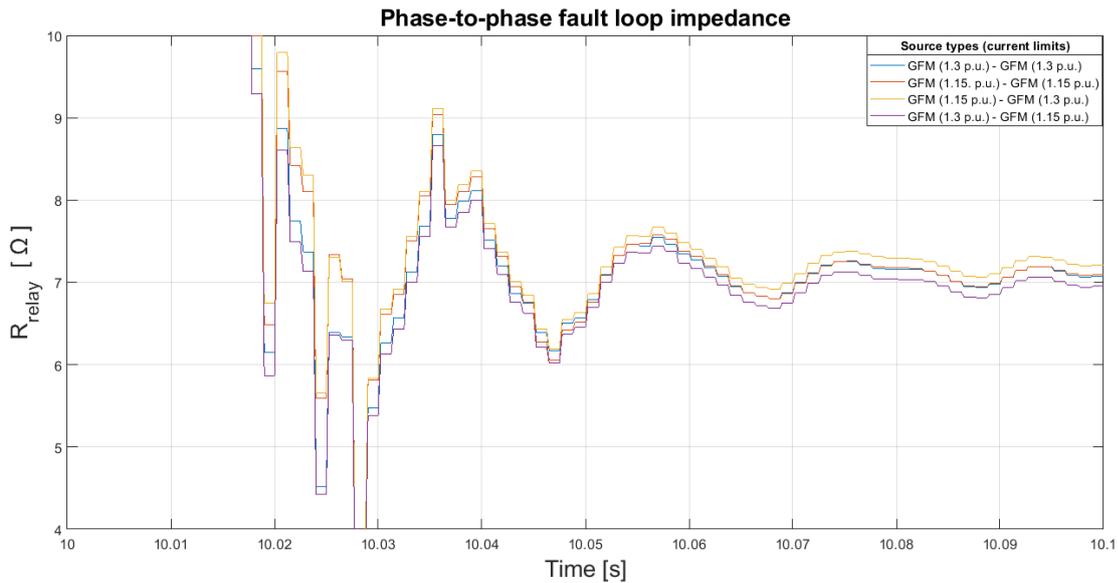
**FIGURE 3-26: VARIATIONS OF THE CURRENT LIMITS, SAMPLED 40 MS LATER (86 KM LINE).**



**FIGURE 3-27: VARIATIONS OF THE CURRENT LIMITS, SAMPLED 40 MS LATER (20 KM LINE).**

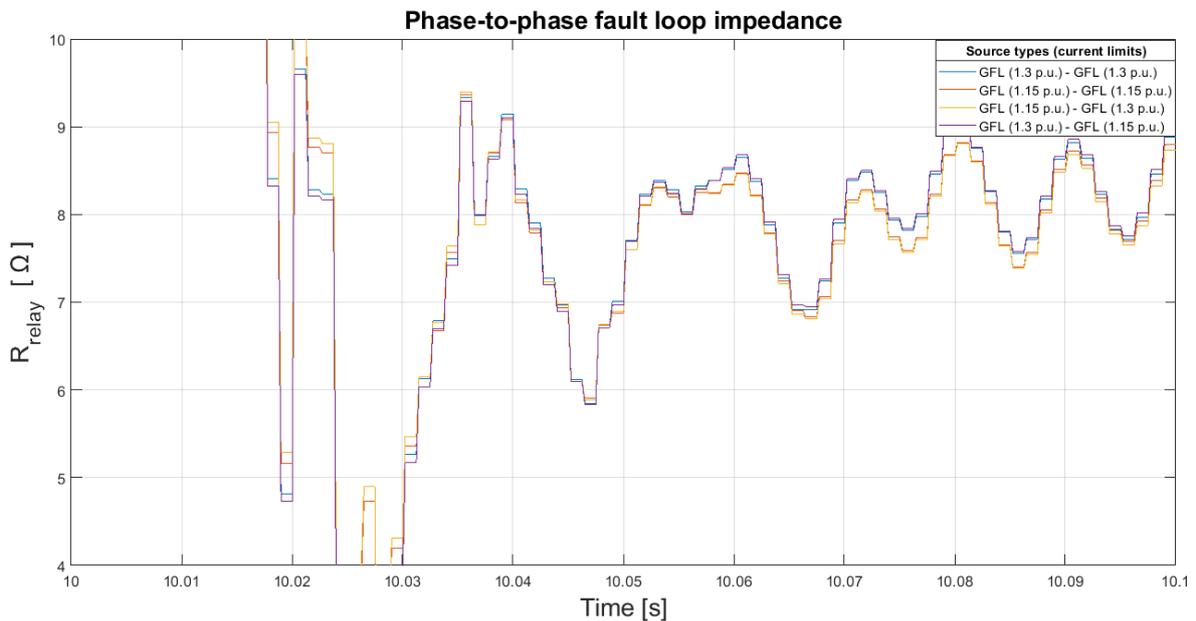
Here, a situation similar to the previous results from the 20 km line model, presents itself regardless of line length. When looking at the GFMs, it is easy to understand the results obtained. By the same argument as was used for the initial divergences for the bandwidth simulations, the factor  $\mu$  for the fault-loop impedance is the determining factor.

By evaluating the factor  $\mu$ , it can be asserted that comparative changes in both the current limits of the GFMs causes  $\mu$  to remain constant (at least magnitude-wise). Similarly, asymmetrical changes in the current limit should cause the magnitude of the impedance shift to slightly increase or decrease. This is corroborated by the transients from the GFM simulations in the 86 km model, presented in Figure 3-28. The fault occurs at  $t = 10$  s.

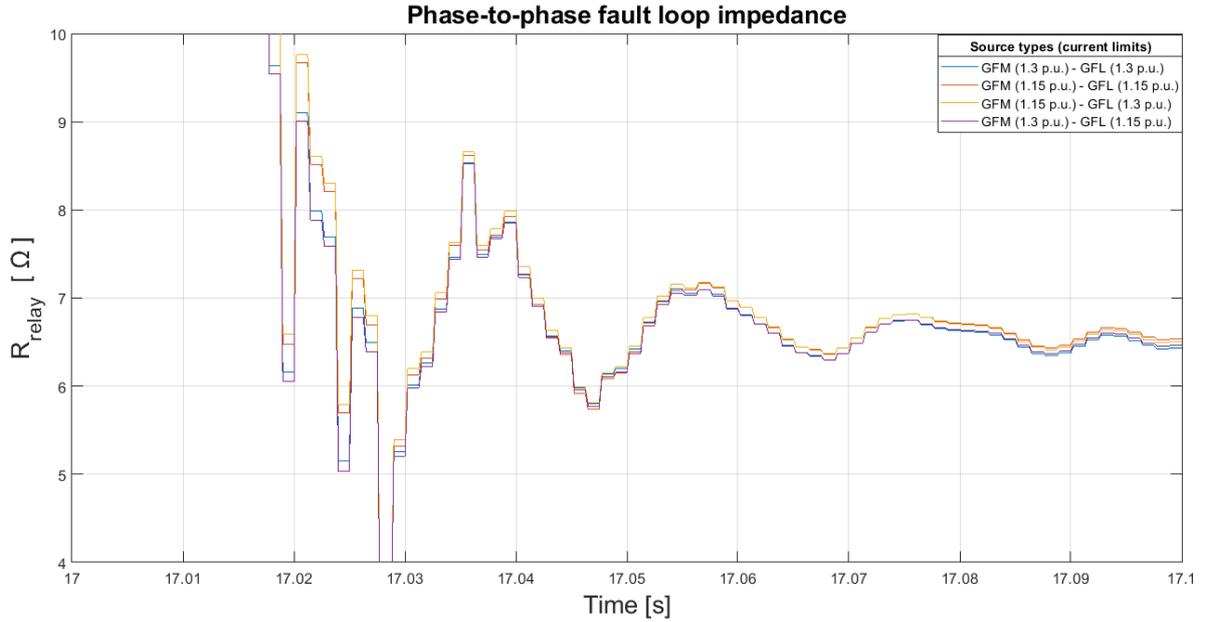


**FIGURE 3-28: FAULT-LOOP RESISTANCE BETWEEN TWO GFMS (CURRENT LIMIT VARIATIONS).**

After an initial transient, the resistances for the simulations where both GFMs have the same current limit (p.u.) converge. Appropriately, when the GFM near the fault has a limit of lowered current limit, the resistance has increased, in accordance with the equation (3.5). The opposite happens when the GFM near the fault has 1.3 p.u. and the second a limit of 1.15 p.u. The transient results for the two-GFL and the GFM/GFL configuration are pictured in Figure 3-29 and Figure 3-30, respectively.



**FIGURE 3-29: FAULT-LOOP RESISTANCE BETWEEN TWO GFLS (CURRENT LIMIT VARIATIONS).**



**FIGURE 3-30: FAULT-LOOP RESISTANCE BETWEEN A GFM AND A GFL (CURRENT LIMIT VARIATIONS).**

In both cases, the magnitude of the measured fault-loop resistance correlates with the current limit of the converter close to the fault. A potential cause for this behaviour, is the GFLs behaving as a current source. In order to test this hypothesis, a modification of the GFM is conducted.

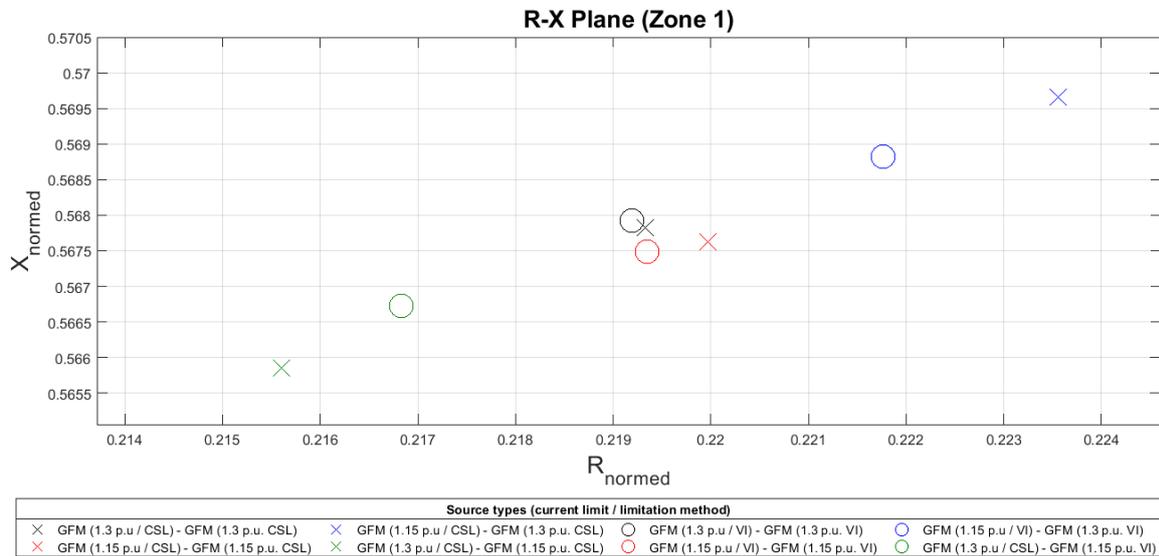
### Virtual Impedance-based current limitation

As GFMs and GFLs behave as different types of sources in the grid, it is difficult to test the hypothesis above. However, as suggested by the available literature, using an alternative method of current limitation may lead to some insights. To this end, a basic implementation of Virtual Resistance (VI) current limitation is implemented. This replaces the current saturation limiter in GFMs. Whereas previously the reference being fed into the current controller of the GFM was limited, VI limits the reference signals fed into the voltage controller directly. Additionally, the presence of a virtual resistance  $R_v$  and  $L_v$  is assumed. The derivation of the reference signals for the LCL-filter capacitor voltages is then modified as follows [35]:

$$\begin{cases} e_{ref}^p = v_{droop} + i_i^q(L_i + L_v) - i_i^d(R_i + R_v) \\ e_{ref}^q = -i_i^d(L_i + L_v) - i_i^q(R_i + R_v) \end{cases} \quad (3.10)$$

For the purposes of this test, the R/X quotient of this virtual impedance was set to be equal to that of the line impedances. The magnitudes of these virtual impedances were increased by trial-and-error until the desired current limits were observed. The presence of the VI cause the GFM to behave as a limited current source during the fault, as the limitation of the voltage reference signals reduces transients observed with the current saturation limiter [35]. The simulations with the 86 km line configuration were repeated. The results obtained are pictured in Figure 3-31. The VI displayed slightly lesser deviations during the asymmetrical configurations in the current limits, however the fault-loop impedances of the configurations with symmetrical current limits converged here as well. It can therefore not be claimed that it is the behaviour of GFLs as a current source which directly cause the effects observed above.

The most likely answer therefore, is that the cause for the outcome observed is the requirement of the GFL at bus three two follows the voltage signal of the grid. Both in configurations with two GFLs and a GFM/GFL combination, the converter located near the fault experiences a larger voltage drop and may therefore dictate the behaviour of the other GFL. The two GFMs, due to being able to generate their own voltage signal, do not exhibit this behaviour. Further research into this behaviour should be conducted.



**FIGURE 3-31: COMPARISON BETWEEN CURRENT SATURATION LIMITING (CSL) AND VIRTUAL IMPEDANCE (VI) IN TWO GFMS.**

As these are the prevalent control concepts found in converters today, especially in onshore applications, they are highlighted as potential sources of false detection in the context of distance protection. In Table 3-3 an overview of the general outcomes observed is provided. Across all simulations, faults occurring between two GFLs show the most severe outcomes due to the impedance shift in both magnitude and phase. This is further influenced by variations in line length, fault type, or the position of the source within the grid. When examining faults between two converters with different line lengths, it was observed that faults closer to the protection and on shorter lines are more prone to false detections. As previously explained, this is a result of the proportion of fault impedance to line impedance.

**TABLE 3-3: INFLUENCING FACTORS ON THE DISTANCE PROTECTION RELAY.**

	GFM + GFM	GFM + GFL	GFL + GFL
<b>IMPEDANCE SHIFT (MAGNITUDE)</b>	Displayed the least amount of shifting across most simulations, possibly due to the effect of primary controllers in both converters.	Displayed similar amounts of shifting as the GFM + GFM simulations. Some variations due to transient processes were observed.	Displayed more severe impedance shifts across all simulations due to the converters behaving as current sources and the accompanying transients.

<b>IMPEDANCE SHIFT (PHASE)</b>	Displayed various amount of phase shifting. The effects on distance protection were minimised by generally low magnitudes of the impedance shift.	Displayed similar phase shifts in the measured impedance as the GFM + GFM simulations. This comes as a consequence of the GFL following the GFM voltage signal.	Displayed impedance shifts in various directions depending on the boundary conditions. The shifts are the most severe due to higher magnitudes of the shifting.
<b>INFLUENCE OF FAULT TYPE</b>	Severity of the outcomes is linked to the fault type (balanced vs unbalanced, grounded vs ungrounded) since the GFM model is only able to provide balanced currents.	Similar changes in severity between the fault types as the GFM + GFM simulations, suggesting that the GFM behaviour dominates.	Matching order of severity of fault types to other converter combinations. However, the impedance shifts increased by a larger amount compared to simulations with a GFM present.
<b>INFLUENCE OF LINE LENGTH</b>	Smaller impedance shifts as line length increased, due to smaller ratios of the fault impedance to the line impedance.	Smaller impedance shifts as line length increased, due to smaller ratios of the fault impedance to the line impedance.	Smaller impedance shifts as line length increased, due to smaller ratios of the fault impedance to the line impedance. Differences in transients become less relevant as line length increases.

By and far, when examining faults between two converters, the most important determining factor for the direction in which the fault-loop impedance is shifted is the type of control structure deployed by the converters. In all simulations conducted here, adjusting control design parameters only caused slight variations in the fault behaviour transients and the fault-loop impedance shifts. Overall, the characteristic of the impedance shift was still chiefly determined by whether there were GFMs, GFLs, or a combination of both present near the fault. Furthermore, it was observed that in the time range which is relevant for protection (first few 10s of ms after a fault), in the case of the converters being fully saturated after a fault occurs, even the presence of transients and oscillations did not overshadow the type of converters as an influencing factor. Given prior information on the fault behaviour of the converters in a grid, adjustments in control design parameters such as bandwidth or the allowed current limit can be predictably evaluated as a potential problem source. Specifically, adjustments to the bandwidth of the PI controllers are highlighted as a potential problem source, as even though the changed transients they introduced disappear after less than 100 ms in the concrete case, it is precisely this time-range that is critical for the protection of AC grids.

### D3.3: Protection Concepts

In chapter 0 the conclusion as well as recommendations are outlined.

## 4. Cyber Security Events

Power systems are undergoing fundamental changes in terms of digitalization, decarbonization, and decentralization. The realization of these trends has necessitated the widespread adoption of novel digital technologies, resulting in cyber security concerns [61]. Hence, power grids are now more susceptible to cyber-attacks as a direct result of their growing reliance on digital technologies and equipment. Attacks on the power grid can potentially lead to devastating consequences for public safety, national security, and economic stability. Therefore, the cyber security of power grids has emerged as a critical issue that is being widely investigated in academic research [62].

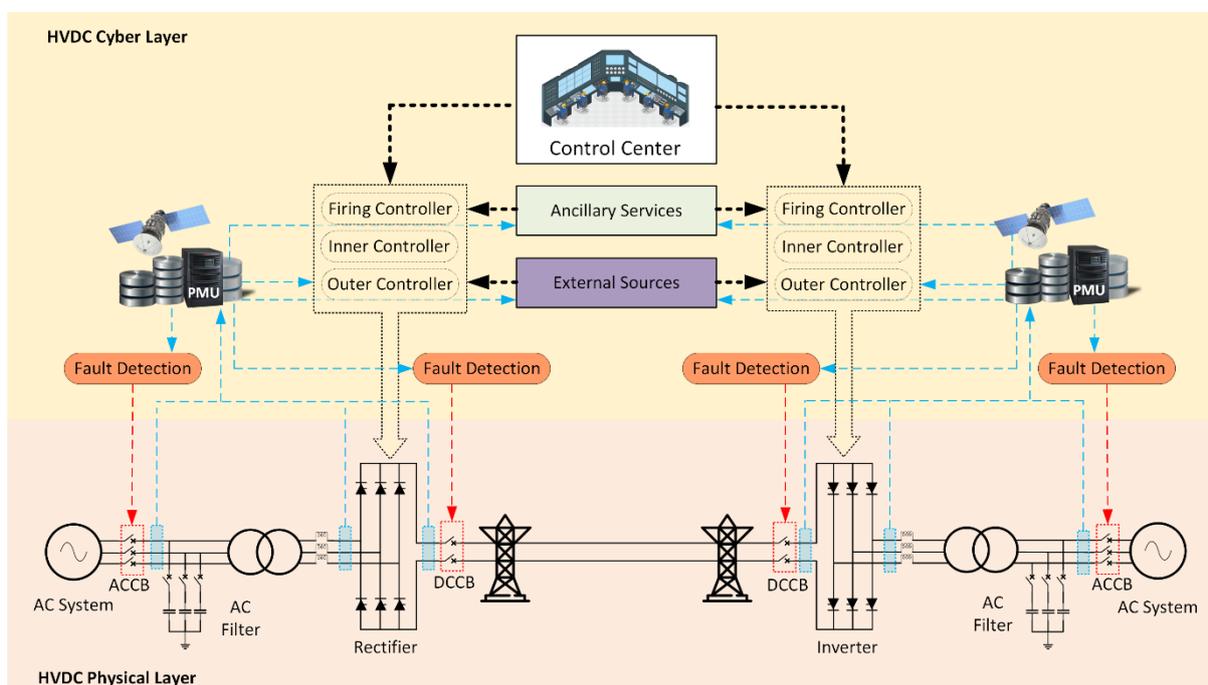
The state-of-the-art research is currently examining the cyber vulnerabilities of new prominent technologies being integrated into power grids, assessing the impact of cyber-attacks on their operation, and creating defense strategies to protect them from attacks. The research includes state estimation and automatic generation control [63], [64], optimal power flow [65], [66], cyber security for Phasor Measurement Units (PMU) [67], [68], and power system communication protocols [69], [70]. Among that research themes, the investigation of cyber security of High-Voltage Direct Current (HVDC) systems have become increasingly popular [71]. While there has been extensive research on cyber security aspects of High-Voltage Alternating Current (HVAC), there is no research specifically focused on the cyber security aspects of HVDC.

In the present section, we unveil vulnerabilities of HVDC-HVAC systems to cyber-attacks. This insight shall allow identifying trustworthy ways of performing anomaly detection based on power system measurement data and operational technology (OT) traffic for HVDC-HVAC cyber-physical systems. HVDC-HVAC cyber-physical co-simulation is used to investigate the impacts of cyber-attacks on the HVDC system. Case studies of cyber-attacks were implemented using the Real Time Digital Simulator (RTDS) and Hardware in the Loop (HIL) facility within the ESP lab at TU Delft. In addition, state-of-the-art cyber-attack mitigation strategies are discussed alongside our proposed anomaly detection method. The proposed method provides a quantitative assessment of communication traffic throughput of HVDC Operational Technology (OT) using hybrid deep learning and attack graph model.

### 4.1. Cyber-Physical HVDC System

The traditional power system is evolving into a large cyber-physical system due to the increasing integration of communication network technologies. This section provides an explanation of how an HVDC system might be regarded as a cyber-physical system. Fig. 4.1 depicts a high-level conceptual architecture of cyber-physical HVDC systems. As shown in Fig. 4.1, HVDC systems are made up of different physical layer components. The converter station serves as the backbone of an HVDC system, converting AC voltage to DC voltage (rectifier mode) or vice versa (inverter mode). Line Commutated Converters (LCCs) and Voltage Source Converters (VSCs) are the two most common technologies used in HVDC converter stations. The converter transformer serves as an interface between the alternating current and direct current systems, as well as a means of isolating the converters from any short circuit failures on the alternating current side. Furthermore, multiple AC filters and reactors are often installed in HVDC stations to reduce harmonics. On the AC/DC side of the converters, AC circuit breakers and, prospectively, DC circuit breakers are utilized to protect the system against short circuit faults. Different HVDC transmission configurations (e.g., monopolar, bipolar, etc.) are used around the world. It should be emphasized that the choice of these designs and other physical component specifications is mostly determined by the unique demands and requirements of the individual HVDC system.

According to Figure 4-1, the interactions between various components of the cyber layer are more complex than those of the physical layer. To begin, Supervisory Control and Data Acquisition (SCADA) measurement devices collect high-speed synchronized samples of various grid variables (such as AC and DC side voltages, currents, and powers) from the system. The measurements collected at each HVDC station are used by the appropriate HVDC terminal controller to create proper firing angles for the converter. The HVDC terminal controller is composed of several layers. The outer controller is in charge of generating reference values for the interior layers by taking into account one or more targets (such as active and reactive power control, AC and DC voltage regulation, etc.). The inner controller is in charge of regulating the current that flows through the phase reactor. This is typically accomplished through the use of the decoupled dq-current control architecture. Finally, utilizing techniques such as Pulse Width Modulation (PWM), the firing controller generates the firing logic for the converter switches. To improve the overall system controlling performance, two-way communication between HVDC station terminal controllers is frequently present.



**FIGURE 4-1: HVDC CYBER-PHYSICAL SYSTEM.**

HVDC systems can also provide power grid ancillary services such as power oscillation damping, frequency regulation, etc. There are some algorithms that employ the PMU readings from both HVDC stations, and appropriate control actions are subsequently delivered to the terminal controllers. The PMU measurements and ancillary service are also supplied to the HVDC control center or DC substation, which controls the converter station, which controls the converter station. Subsequently, the information is processed to make corrective actions to improve the overall operation of the power grid. These decisions are sent to HVDC terminal controllers and associated services in a variety of ways, including power order commands. Some external sources (for example, Remedial Action Schemes) may also offer input data for terminal controllers. AC and DC fault location algorithms process the measurement device data to determine the occurrence of faults in the system and send appropriate tripping signals to the AC and DC circuit breakers.

According to what has been mentioned thus far, cyber layer components play an important role in the control and protection of HVDC systems. However, the many cyber layer components shown in Figure 4-1 typically connect with one another via well-known unsecure communication protocols like as

DNP3, IEC 60870-5-101/104, and IEC C37.118 [72]. Investigating the cyber risks of HVDC systems is therefore critical for ensuring their secure operation and control. For this reason, the objective of this sub-section is to investigate the cyber threat and vulnerabilities of HVDC systems.

## 4.2. Cyber Threats and Vulnerabilities on HVDC

Existing state-of-the-art research on HVDC cyber security mainly focused on three categories of cyber-attacks targeting various HDVC systems components, i.e., including False Data Injection Attacks (FDIAs), Replay and Spoofing Attacks, and Denial of Service (DoS) attacks. These attacks aim at driving AC/HVDC systems in unstable conditions, causing large frequency deviations and oscillations possibly leading to widespread blackouts, reducing power quality, and drastically affecting overall system performances and efficiency. To cause this impact on the grid, the attacks specifically target different types of converters, i.e., LCC, VSC, and specifically MMC-VSC, and control functions, including LFC, damping control, and other ancillary control services used in HVDC systems. Table 4-1 shows a summary of targeted system components and attack types identified from the state-the-art literature review. The following part will discuss the attacks and vulnerabilities and impacts on HVDC system.

**TABLE 4-1: SURVEY ON CYBER-ATTACKS TARGETING HVDC SYSTEMS COMPONENTS.**

TARGETED SYSTEM	ATTACK TYPES	REFERENCES
Voltage Source Converter (VSC)	FDIA	[73], [74], [75], [76], [77], [78]
	DoS	[73]
Line Commutated Converter (LCC)	FDIA	[79], [80], [81], [82]
	Dos, Replay Attack	[79]
Modular Multilevel Converter (MMC)	FDIA	[77], [83], [84]
	DoS	[85], [86]
Load Frequency Control (LFC)	FDIA	[76], [87], [88]
	DoS	[87]
HVDC Ancillary Control and Services	FDIA	[89], [90], [91], [92], [93]
	Dos, Replay Attack	[90], [91], [93]

### 4.2.1. False Data Injection Attacks

The most common approach to maliciously manipulate HVDC systems' behavior is FDIAs. FDIA involves the injection of malicious or manipulated measurement data regarding the state of the electrical power grid. These measurements may be acquired by Remote Terminal Units (RTUs), collected and aggregated by Phasor Data Concentrator (PDC), delivered to Supervisory Control and Data Acquisition (SCADA) systems, and finally used by state estimation and control algorithms to monitor and operate the grid effectively. If the communications between the components are not protected appropriately, for instance by using secure authentication and encryption techniques, the attacks can be executed by mining the integrity of the messages exchanged between PMUs and PDCs or between PDCs and HVDC systems [91]. Further, these kinds of attacks can remain stealthy and circumvent the regular bad data detector systems if the attacker has enough resources or knowledge of the system under attack [87], [88].

As discussed in [91] and [92], different attack approaches can be adopted to tamper with the reported measurements, including (1) False Oscillation Attack, (2) Ramp Attack, (3) Scale Attack, (4) Data Interchange Attack, and (5) Playback Attack. Moreover, FDIA attacks can also be characterized in terms of magnitude, duration, and template of the injected false data. Examples of attack templates are provided in [93] where the data modification takes the form of an added bias, gradient, pulse, or noise, or the scaling and sign inversion of the measurements. These different attack approaches have the objective to maximize the attack impact while minimizing the probability of being detected by bad data detectors and other defense mechanisms. Depending on the targeted system and on the intruder's desired outcome, the choice of the manipulated quantity can vary, including voltage, frequency, and power measurements.

Different studies focused on FDIA attacks targeting Line Commuted Converters (LCC). Attacks to LLC systems have been studied in [70], and by conducting simulation it has been shown that FDIA on the rectifier or inverter sides of HVDC systems operated in DC control mode can limit the power transmission or cause instability in the system. Further, it is also shown that FDIA on the inverter side of HVDC system can result in communication failures which can lead to a decrease in the inverter efficiency or damage to the device.

Other studies present FDIAs on Voltage-Source Converters (VSCs). When FDIAs are performed to VSC, the voltage measurements of one or multiple grid buses can be tampered with to deteriorate the stability of the system, increase switching losses, and consequently decrease the efficiency of the HVDC systems [74]. In [78], a cyber-attack tampering with the reported active power to VSC is analyzed, and it is shown how the attack can lead to a biased transmission power and result in a frequency deviation in AC grids and voltage deviation in DC grids, which consequently threatens the secure operation of the hybrid AC/DC grid. Various combinations of FDIA tampering with AC and DC voltage and power measurements can be used to attack VSC Multi-terminal HVDC systems as presented in [75]. Moreover, as shown in [73], attacks can aim at manipulating the various reference values incorporated in VSC control strategies in order to alter the controller behavior.

Different studies explore FDIAs on Modular Multilevel Converters (MMC). In [84], an MMC controlled by a consensus-based distributed control scheme is considered, and the authors show how, by targeting the submodules' capacitor voltage balancing control mechanism. It is possible to cause an increase in the capacitor voltages and the tripping of the submodules for overvoltage protection. In [77], the authors focused on attacking MMC controller parameters and demonstrated how attacks to the parameters of PI controller in the voltage controller, current controller, and PLL can cause a significant increase in controller overshoot and steady-state error, and high oscillation behaviors. Also, the authors in [83] concluded that an attacker can move the system closer to instability margins by tampering with either the measurements or reference values used by the MMC controller.

Regarding the control part of HVDC systems, damping control and Load Frequency Control have been proven to be vulnerable to FDIA attacks [76]. Indeed, in [89] it is analyzed how the manipulation of frequency measurements can cause low-frequency inter-area oscillations, by forcing the controller to increase the output power to damp the falsely reported frequency oscillation, still aggravating the system stability and increasing the frequency deviation. In [90], it has been discussed that voltage magnitude and angle manipulation can affect the system's stability. The impact of tampering with power and frequency measurements reported to LFC is further explored in [87] and [88], where the authors further show that LFC systems with AC/HVDC interconnection and emulated inertia can be more vulnerable to FDIA compared to the ones without inertia emulation and normal AC systems.

## 4.2.2. Replay and Spoofing Attacks

A replay attack refers to a form of network attack in which an attacker intercepts and captures valid data that are being exchanged between two entities, such as authentication credentials or data packets. The attacker then replays these captured data at a later time to impersonate the original sender or gain unauthorized access to a system or network. Replay attacks take advantage of the reuse of unaltered valid data, circumventing security measures and potentially resulting in unauthorized actions or the disclosure of information. Unlike replay attacks, spoofing attacks involve not only capturing data but also modifying them before sending them to the target. Spoofing is an active attack where adversaries pretend to be legitimate entities and disrupt normal communications. Such attacks can be realized through many forms of spoofing such as emails, website URLs, text messages, Global Positioning System (GPS), and IP addresses.

In the HVDC grids, replay attacks aim at deceiving state estimation and control algorithms, but instead of injecting malicious or manipulated measurements, they rely on the retransmission of valid signals that have been previously intercepted by monitoring the communication channel. Given that the replayed signals are contained invalid messages, if proper prevention and detection mechanisms are not implemented, the repeated messages are going to be accepted by the receiving system [93]. This type of attack has been studied in [79] adopting two different approaches; in the first approach the frequency measurements are intercepted during severe transient event and then replayed during normal operations to the damping controller, whereas, in the second one, the measurements are recorder while no system disturbances are present and then re-transmitted when a large system transient event exhibits. With these approaches, it has been shown how the Replay Attack can trigger interarea oscillation in the system or disturb, or even disable, the normal operations of the HVDC damping controller. Replay attacks can also be performed in combination with other types of malicious behavior to cover up the ongoing disturbances, and thus avoid the monitoring and control systems response [91]. In [91], Replay Attacks are performed in combination with FDIA and Denial of Services (DoS) attack to deceive HVDC Ancillary Service Control (HASC) and cause false control.

This report performs a spoofing attack on Generic Object-Oriented Substation Event (GOOSE) traffic which controls the HVDC grids. The first stage of the attack model is to monitor the substation communication traffic and identify GOOSE. The structure of standard GOOSE frame is shown in Figure 4-2. The common fields include, the physical link destination and source addresses, i.e., Media Access Control (MAC), tag of the Virtual Local Area Network (VLAN), type header, length of the frame, and data payload. For a typical GOOSE frame, under the data payload, the data set contains the various trips commands and breaker statuses. The status and sequence number fields, i.e., StNum and sqNum, are important from an operational perspective. In the processing algorithm of GOOSE messages, the sequence number is incremented continuously with every GOOSE message sent while the status number is fixed. The status number is changed by one in the case of an event in the relay, e.g., a relay trip, and the sequence number is reset to zero. Thus, GOOSE messages with a lower status number are discarded. Due to the lack of cyber security implementations, GOOSE is susceptible to man-in-the-middle cyber-attacks. Spoofed information can be supplied to the protection Intelligent Electronic Devices (IEDs) to trigger or inhibit protection functions. Figure 4-3 shows the comparison of normal GOOSE frame and spoofed GOOSE frame.

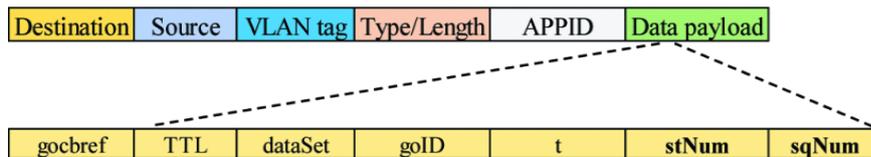


FIGURE 4-2: STRUCTURE OF GOOSE DATA FRAME

Normal operation GOOSE frame	Cyber attack: Spoofed GOOSE frame
gocbRef: P446_SVSystem/LLN0\$GO\$gcb01	gocbRef: P446_SVSystem/LLN0\$GO\$gcb01
timeAllowedtoLive: 2001	timeAllowedtoLive: 5
t: Mar 28, 1994 03:42:25.531999945 UTC	t: Mar 20, 1994 22:04:09.076999962 UTC
stNum: 95	stNum: 99
sqNum: 80850	sqNum: 0
numDatSetEntries: 10	numDatSetEntries: 10
allData: 10 items	allData: 10 items
Data: boolean (3)	Data: boolean (3)
<b>boolean: False</b>	<b>boolean: True</b>

FIGURE 4-3: COMPARISON OF NORMAL AND SPOOFED GOOSE FRAME.

### 4.2.3. Denial of Service

Denial-of-Service (DoS) is a cyber-attack with the objective of preventing legitimate access for users / networked devices to specific system resources such as network connections, computing capabilities, and application services. The term distributed denial-of-service (DDoS) refers to a coordinated DoS attack originating from multiple, distributed sources to increase attack severity and prevent tracking and identification of attackers’ origin. A single DoS attack can be mitigated by blocking the sole attack source. Conversely, for a DDoS attack, blocking all attack sources is challenging, making its mitigation difficult.

In HVDC grids, DoS aims at limiting or blocking the communications between data sender and receiver, obliging control and SE algorithms to operate on outdated data, thus affecting at least the accuracy of control signals. Multiple studies analyzed the impact of DoS attack to HVDC systems, targeting VSC [73], Line Commutated Converters (LLC) [79], Modular Multi-level Converter (MMC) [85], [86], Load Frequency Control (LFC) [87], and Automated Generation Control (AGC) and Power Modulation Controller (PMC) [93]. Further, in [85] the authors analyze three different types of cyber delay in MMC-HVDC that, if caused by a cyber-attack, can lead to a DoS; the considered attack points to the data life cycle are: sampling and data processing, signal modulation, and signal transmission. As for the previously discussed attacks, also DoS attacks to HVDC systems can create stability issues, outages, and appliance damage, but in this case, it is particularly difficult to design and deploy effective countermeasures given the intrinsic nature of the attack.

## 4.3. Cyber-Physical HVDC Co-Simulation

Power grids are a critical infrastructure that must meet stringent requirements for availability. Conducting tests and experiments on actual power grids is unfeasible. Therefore, Cyber-Physical System (CPS) modelling and simulation are required to assess the system vulnerability and cyber attack impacts on the power system. Power system simulation can be integrated with IT and Operational Technology (OT) system simulation to create co-simulation. The co-simulation provides a more

realistic result by considering both aspects of cyber and physical systems. The state-of-the-art power system modeling and co-simulation are presented in a number of survey papers that can be found in [94], [95]. However, all of them are focused on general power systems rather than HVDC systems. Therefore, in this report, we identified the state-of-the-art CPS co-simulation model for HVDC and explain our HVDC co-simulation setup.

### 4.3.1. State-of-the-Art HVDC Model and Co-Simulation

The state-of-the-art from HVDC co-simulations are summarized in Table 4-2. The table identifies the power system model used to simulate the HVDC system, tools for the power system simulator and the IT/OT simulator. There are baseline power system models that have been modified by incorporating HVDC elements from 4 bus up to 118 bus models. The models are in line with the current real-world power system, which is primarily based on HVAC but is gradually incorporating HVDC technology. To simulate the power grids under the cyber-attack scenarios, the state-of-the-art research uses power system simulators. The simulator tools include Matlab Simulink, Power Systems Computer Aided Design (PSCAD), Real-Time Digital Simulator (RTDS), and Piecewise Linear Electrical Circuit Simulation (PLECS). Among those power system simulators, Matlab Simulink is the most popular power system simulator because of its versatility in model implementation. However, from a fidelity standpoint, PSCAD and RTDS offer superior performance due to their electromagnetic transient capability.

**TABLE 4-2: SURVEY ON HVDC CO-SIMULATION.**

REF.	YEAR	POWER SYSTEM MODEL	POWER SYSTEM SIMULATOR	IT/OT SIMULATOR
[77]	2023	Two-terminal MMC–HVDC system	Matlab Simulink	-
[96]	2022	16-machines 68-bus with VSC based HVDC	Matlab Simulink	-
[97]	2022	10-machine 39-bus onshore AC system	Matlab Simulink	-
[98]	2022	two-area power grid with HVDC	Matlab Simulink	-
[99]	2021	16-machines 68-bus AC/DC hybrid power system	Matlab Simulink	-
[27]	2021	Kundur's two-area system	RTDS	VIRTUAL PMU SERVER AND PDC COMMUNICATION MODEL
[21]	2021	-	Matlab Simulink	COMMUNICATION MODEL
[86]	2021	IEEE 12-bus AC/DC test system	Matlab Simulink	-
[83]	2021	-	Matlab Simulink	-
[100]	2021	-	Matlab Simulink	-
[101]	2021	Two bus HVDC system	Matlab Simulink	-
[87]	2020	16-machines 68-bus with VSC based HVDC	Matlab Simulink	-
[88]	2020	10-bus model with HVDC	Matlab Simulink	-
[102]	2020	10-bus model with HVDC	Matlab Simulink	-
[103]	2019	IEEE 39-bus system with HVDC	Matlab Simulink	-
[74]	2014	IEEE 118-bus system	Matlab Simulink	-
[104]	2019	IEEE 9-bus equipped with HVDC	Matlab Simulink	-
[82]	2018	three-area IEEE 39-bus test system	Matlab Simulink	-
[91]	2023	10-bus model with HVDC	PSCAD	-
[92]	2021	INELFE project model	PSCAD	-
[105]	2021	WECC and EI	PSCAD	-
[106]	2020	BPA Micro WECC	RTDS	-
[107]	2023	-	RTDS	-
[84]	2022	-	PLECS	-
[75]	2019	4-bus test system	-	-
[89]	2020	Kundur's two-area system	-	-
[108]	2020	Bipole series multiterminal HVDC	-	-
[81]	2022	multi-infeed HVDC	-	-
[93]	2022	IEEE 39-bus system with HVDC	-	-
[88]	2023	IEEE 14 bus DC grid	-	-
[79]	2018	MODIFIED IEEE 39-BUS AC-HVDC	-	-

According to the literature review, the majority of research for HVDC systems omits cyber system simulations. Therefore, their cyber-attack scenarios on HVDC are only based on the prior assumption

when the adversaries successfully compromise the IT/OT system. Among them, some research has already integrated IT/OT systems into cyber attack scenarios in HVDC. In [86], the authors incorporate a communication model to assess the stability of the HVDC system. However, this work did not perform actual simulation in the HVDC CPS. Wide-area monitoring, protection, and control for HVDC cyber security were investigated in [106]. The OT simulation incorporates PMUs, PDCs, Intelligent Electronic Devices (IEDs), SCADA systems, and communication links. The OT devices are simulated using Raspberry Pi and virtual servers. Using co-simulation, this research primarily focused on FDIA scenarios. The FDIA detection primarily focused on the analysis of simulated data samples and PMU measurements. Therefore, this implementation is not applicable for more advanced cyber-attacks, i.e., Advanced Persistent Threat (APT).

Based on our review of HVDC co-simulation for cyber security, we have derived the following summary and key points:

- The state-of-the-art cyber-attack simulations on HVDC systems are based on the premise that the IT/OT system has been compromised, allowing the attacker to execute FDIA, Replay, or DoS attacks. The attack scenarios do not resemble the actual cyber-attack on power grids, i.e., Ukrainian power grids in 2015 [109], and 2016 [110]. Furthermore, the simulated cyber-attacks do not comprehensively represent the stages of the cyber kill chain [111]. Therefore, the future co-simulation of cyber-attack on HVDC systems should consider this constraint accordingly to improve the fidelity of the cyber-attack scenarios.
- There is very limited research on HVDC cyber security that implements the comprehensive co-simulation models. Despite the fact that the majority of the research presents a narrative about a cyber-attack on an HVDC system, the studies are primarily concentrated on power systems simulation only. It is crucial to include IT/OT elements in order to create a more thorough simulation of cyber-attacks. Therefore, future research should implement both cyber and physical HVDC systems to present more comprehensive cyber-attack scenarios.

#### 4.3.2. Cyber-Physical HVDC Model and Co-Simulation

In this part, we describe the implementation of cyber-physical HVDC model and co-Simulation. The power system simulation runs on RTDS, and the cyber component runs on real devices as hardware-in-the-loop. The HVDC model simulated in the RTDS is the same as the model of four-terminal terminal MMC-based MTDC network used in Deliverable D3.2 as shown in Figure 4-4. The RTDS configuration for the model implementation is depicted in Figure 4-5. In total the HVDC model runs on 15 Real-Time Digital Simulator (RTDS) cores and 3 racks. Each rack runs different subsystems, i.e., offshore MMC, wind turbines, and onshore MMC.

The hardware-in-the-loop setup used to carry out the cyber-attack investigations is shown in Figure 4-5. The IED 1 is in full compliance with IEC 61850, which enables the relay to process Sample Value (SV) measurements and support GOOSE messaging. The fault condition and trip status are determined based on the received SV input and are then transmitted via GOOSE. IEDs 2 and 3 are partially IEC 61850 compliant. They are inherently connected and receive analog signals from RTDS via power amplifiers. The remaining relays are modeled and simulated using the RTDS. It should be emphasized that all the physical IEDs employed in the HIL setup utilize GOOSE messaging for crucial substation communication, specifically for transmitting trip and block commands via switched Ethernet. This is keeping in line with the concept of a digital substation that employs IEC 61850. Figure 4-6 illustrates the connection of the relay data links to a network switch, which is also connected to the RTDS GT-NET 2x card. The card is connected to the RTDS using an internal optical fiber interface. The card transmits sampled values to IED 1 and receives GOOSE messages from IEDs 1, 2, and 3.

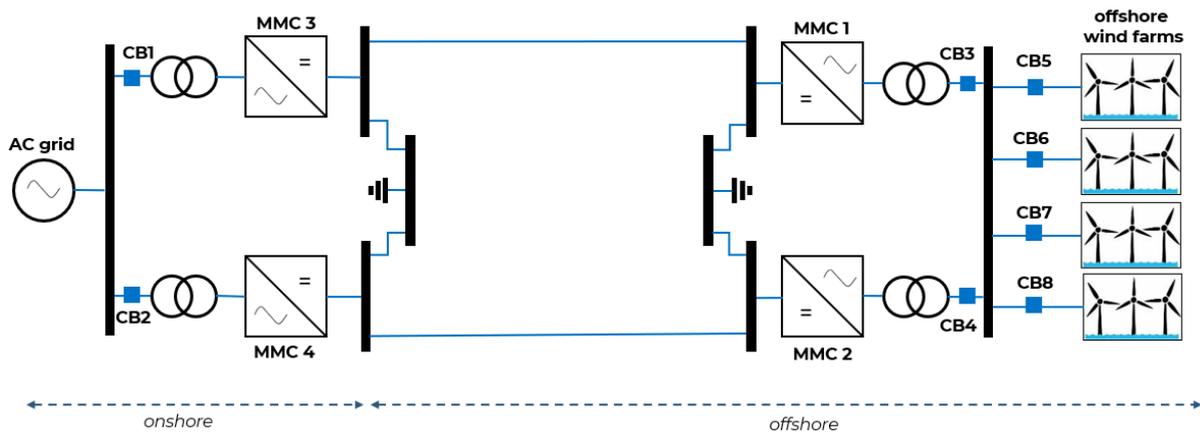


FIGURE 4-4: HVDC SYSTEM MODEL FOUR-TERMINAL TERMINAL MMC-BASED MTDC NETWORK.

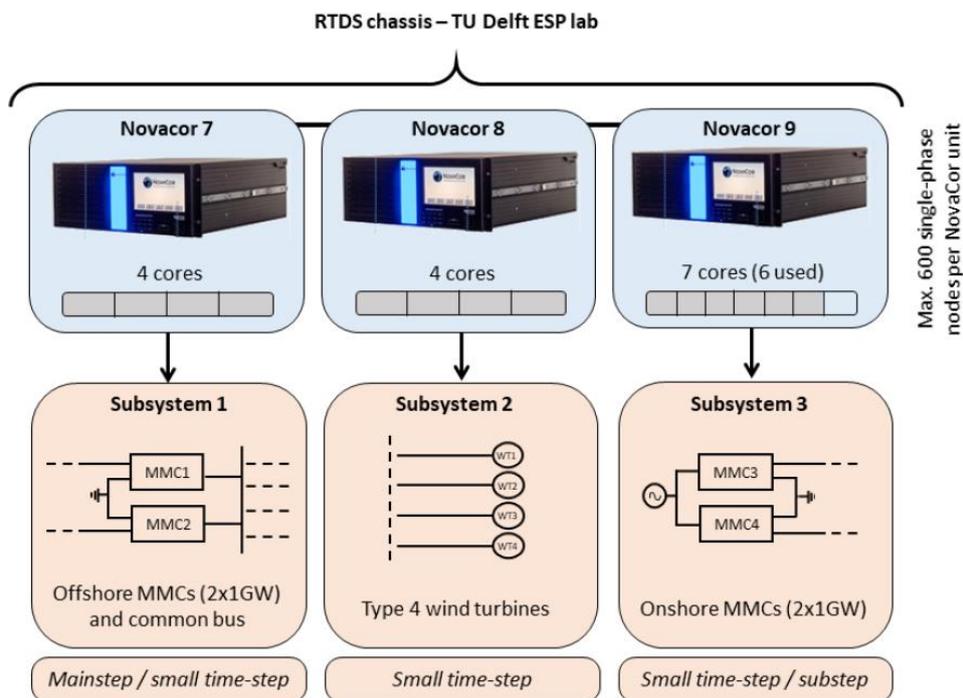


FIGURE 4-5: HVDC SYSTEM MODEL IMPLEMENTATION ON RTDS.

A publisher-subscriber mechanism is utilized by the IEC 61850 standard. In accordance with this mechanism, GOOSE and SV messages are transmitted over the process bus in a multicast fashion using Ethernet. Therefore, a GOOSE message is published to the process bus by a single IED. As opposed to receiving all messages, other IEDs exclusively receive messages that are members of the destination address group to which they are configured to subscribe. Similarly, an IED is programmed to exclusively receive SV measurements from a specific merging unit that is transmitting data to the process bus.

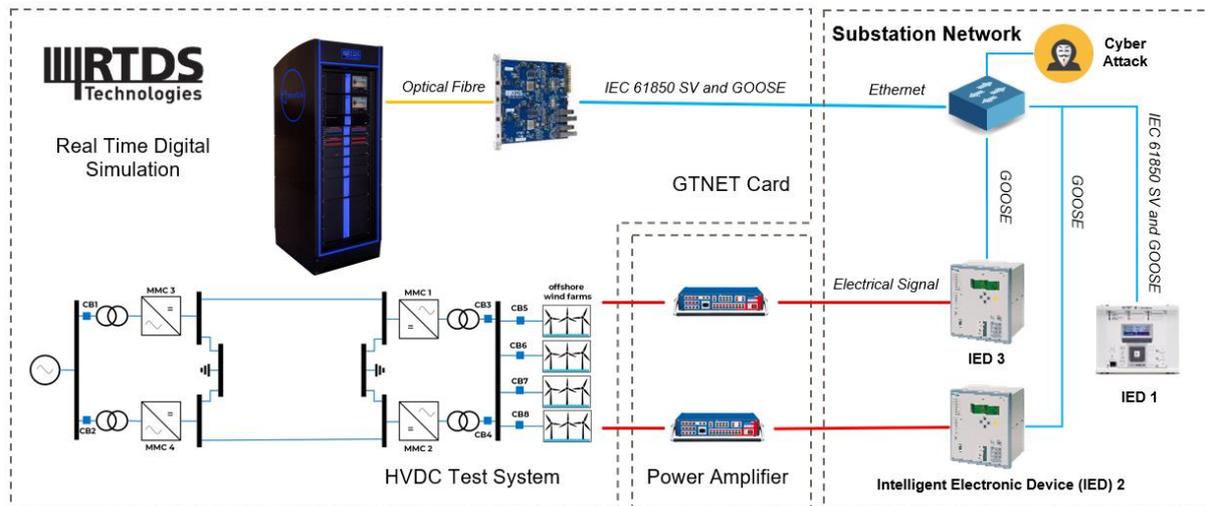


FIGURE 4-6: HARDWARE IN THE LOOP (HIL) SETUP.

### 4.3.3. Cyber Threat Model

A threat model is a systematic and organized representation of various factors and elements that have an impact on the security of an application. It helps to identify, communicate, and comprehend potential threats. An example of a power grid OT network is represented in Figure 4-6. In this study, we assume that an adversary has already compromised a host located in the OT network of a substation. The adversary conducts a cyber-attack on the OT network from the compromised host. In this experiment, we focus primarily on spoofing and DoS attacks. A constrained threat model is used to analyze the OT communication of the power grid.

The network switch depicted in Figure 4-6 represents the substation process bus in this HIL setup. The switch is responsible for both publishing and subscribing to all GOOSE and SV messages. In order to allow for flexibility of connected devices, the switch is configured to broadcast to all accessible ports, meaning it transmits packets to all linked nodes within a single broadcast domain. This is due to the lack of configuration in secure mode. In order to activate this mode, it is necessary to configure flow control rules and restrictions, which have an impact on the network's flexibility and scalability. Hence, adversaries can eavesdrop on crucial substation communication data by acquiring entry to the switch and engaging in packet sniffing. Furthermore, the adversaries can subsequently inject spoofed packets into the network, via the switch. This serves as the foundation for the cyber-attacks in this experiment.

The cyber-attack model proposed in this report is generic and can be executed in two phases utilizing a wide variety of tools. We utilize Wireshark, a widely recognized communication network tool, for the initial stage of network reconnaissance. Wireshark is executed on a different host machine that is linked to the network switch. The network interface of this host machine is configured to operate in 'promiscuous' mode within the Wireshark application. This allows for the monitoring and examination of all network traffic passing through the switch on the host machine. The data obtained from this stage is utilized in a Python script that is utilized on the Scapy networking library. Scapy is a computer network tool that allows for the creation of manipulated data packets or frames. By gaining access to the network switch, the script carries out a man-in-the-middle cyber-attack by injecting spoofed SV and GOOSE data streams directly into the substation communication network. The spoofed SV data streams cause the blocking of protection equipment. This prevents its normal operation during faults. On the other hand, the spoofed GOOSE frames compromise multiple IEDs, causing them to trip and open circuit breakers.

### 4.3.4. Cyber Attack Impact Assessment

As discussed in the previous sections, HVDC systems are susceptible to cyber vulnerabilities that may be maliciously exploited to disrupt system operation. In this sub-section, simulation results from cyber-attack scenarios targeting a HVDC system are presented and discussed. Table 4-3 summarizes all tested scenarios. The normal operation serves as a benchmark/reference for the tested scenarios. The remaining scenarios include DoS attacks, GOOSE spoofing, and AC and DC faults. Based on the HVDC model, the tested anomalies are located in the offshore windfarm, MMC, and DC line. The HIL simulations provide many varieties of data that can be used. In this report, however, the focus is on cyber information from network traffic throughput and power system information from active power (P), current (I), and voltage of MMC 1. MMC 1 and offshore Wind Turbine 1 are selected as the primary measurement points because they are closely connected with the largest offshore power source from Wind Turbine 1. Therefore, the events located in this area result in significant impact.

TABLE 4-3: SIMULATED SCENARIOS.

NO	SCENARIOS	TARGET LOCATION
1	Normal operation	-
2	AC Fault	OFFSHORE WINDFARM FAULT
3	DC Fault	DC LINE FAULT
4	GOOSE spoofing	OFFSHORE WINDFARM CB
5	GOOSE spoofing	MMC 1 CB
6	DoS attack	OFFSHORE WINDFARM CB
7	DOS ATTACK	MMC 1 CB

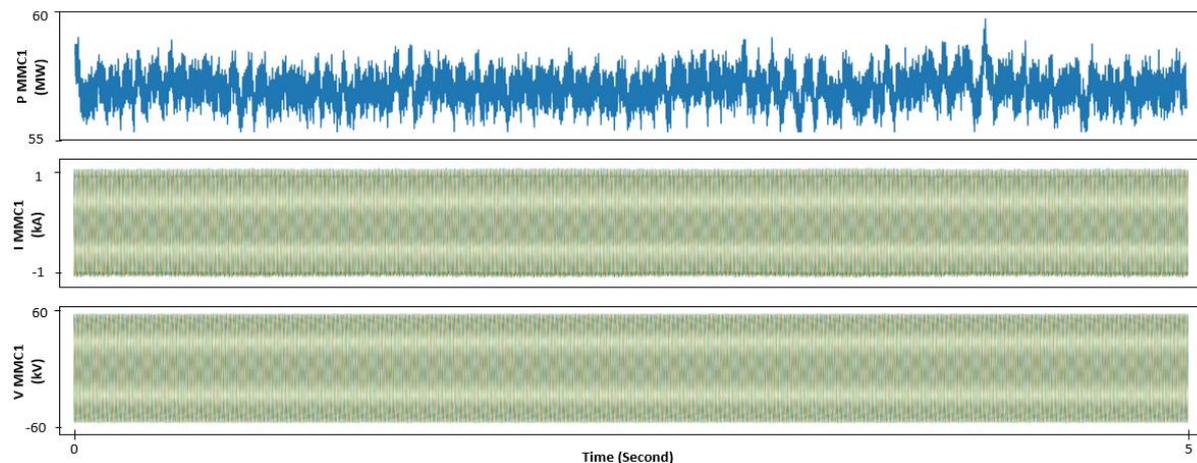
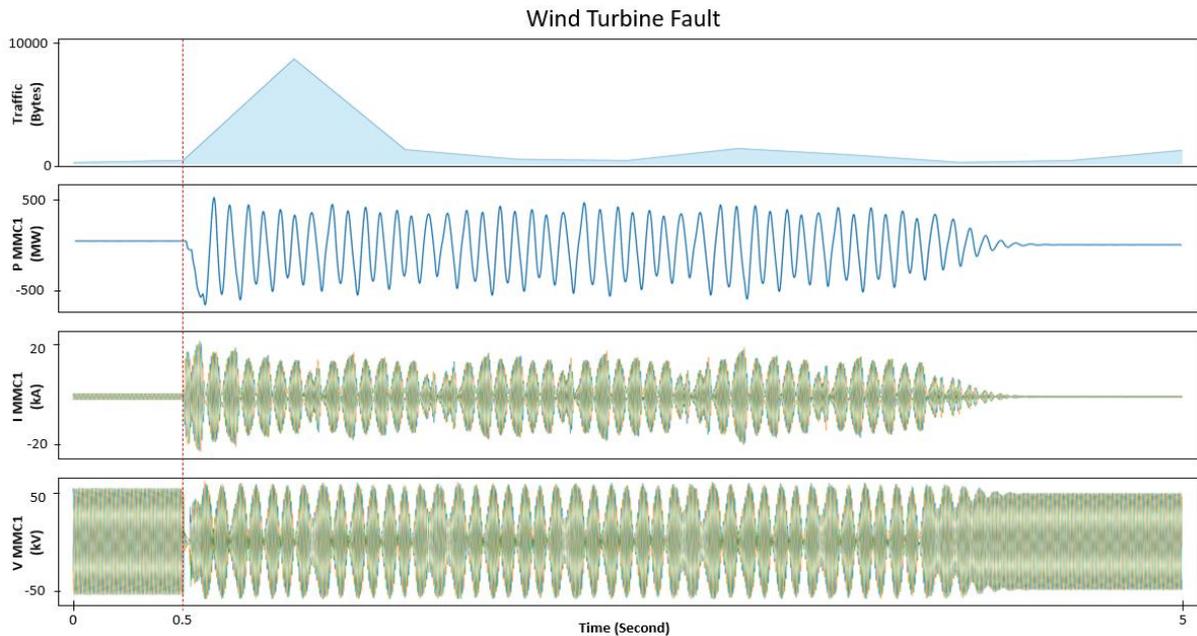


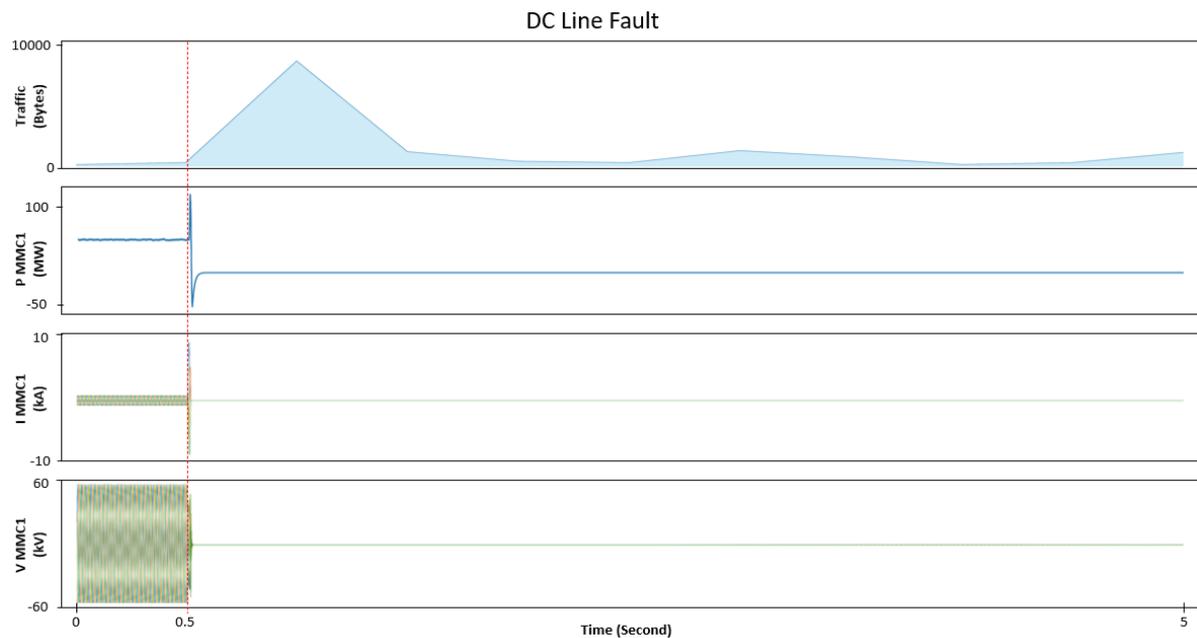
FIGURE 4-7: HVDC SYSTEM UNDER NORMAL OPERATIONS.

Figure 4-7 shows the power system measurements under normal operation mode. The measurements indicate stability of the HVDC simulation. In the simulation scenarios we capture the network traffic and power system measurements every 5 seconds. The measurement of active power (P), current (I) and voltage (V) from the MMC 1 serves as the main reference indicating nominal system operation. Otherwise, the measurements indicate anomalous events. The anomalous events are stimulated at t=0.5 seconds. Figure 4-8 and Figure 4-9 illustrate the impact of faults in the HVDC system. The fault also triggers traffic changes due to protection mechanism. Due to the similar HIL configuration, the traffic anomalies for AC and DC line faults are identical. However, the power system impacts are different. The AC line faults depicted in Figure 4-8 lead to some oscillation in a few seconds until the

system reaches an equilibrium point. Meanwhile, the DC line fault leads to the voltages, currents, and active power in the MMC drop to zero as shown in Figure 4-9.

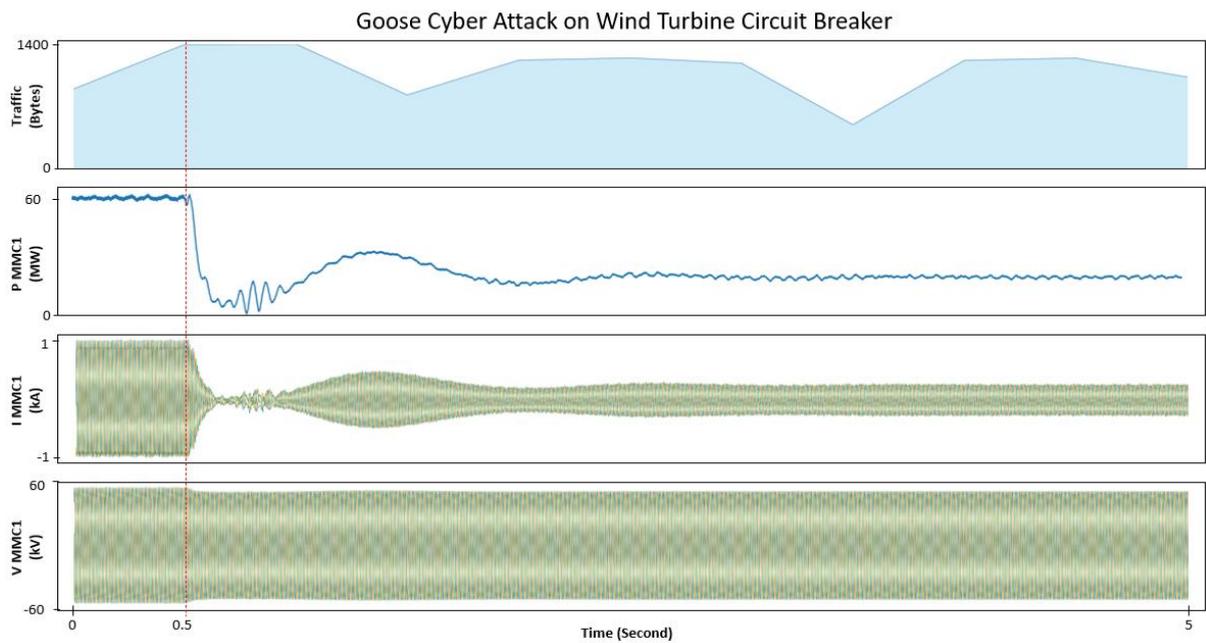


**FIGURE 4-8: WIND TURBINE (AC) LINE FAULT.**

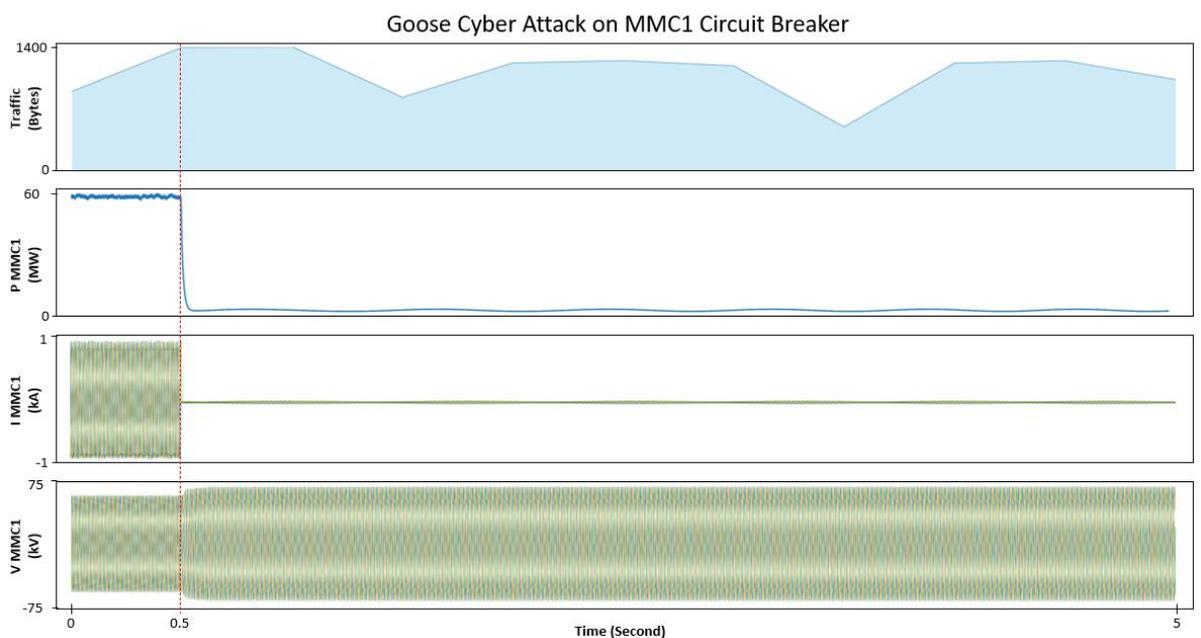


**FIGURE 4-9: HVDC LINE FAULT.**

The impact of GOOSE spoofing attack on different protection relays and circuit breakers located in the wind turbine AC line and MMC 1 is shown in Figure 4-10 and Figure 4-11. Compared to the fault, the spoofing attack triggers less significant traffic anomalies. Subsequently, due to the spoofed GOOSE attack, power system measurements are impacted. Figure 4-10 shows how the spoofing attack on wind turbine AC line leads to P, V, and I to drop. Meanwhile, the GOOSE attack on MMC 1 circuit breaker leads to active power and current drop around zero and slightly increase the voltage. Both of the attacks were caused by malicious opening of circuit breakers using the spoofed GOOSE traffic. However, different locations of circuit breakers lead to different impacts on the power system.



**FIGURE 4-10: GOOSE ATTACK ON WIND TURBINE CIRCUIT BREAKER.**



**FIGURE 4-11: GOOSE ATTACK ON MMC CIRCUIT BREAKER.**

Figure 4-12 illustrates the statistical comparison of traffic from the various scenarios. While the system is functioning normally, the throughput of the traffic is approximately 800 bytes per second. During the GOOSE spoofing attack, there is an observed slight increase in the traffic throughput to 1000 bytes per second. The traffic rate increases to 10000 bytes per second following the occurrence of the fault. These results show that cyber-attacks and system faults result in completely different traffic patterns. The fault results in a rapid tenfold increase in traffic throughput within 0.5 seconds, while the GOOSE attack results in a 40% increase in traffic for only 2 seconds. Meanwhile, the DoS attack results in a sustained increase in traffic for an extended period. These different traffic characteristics are crucial to identify traffic anomalies. Therefore, this report utilizes traffic characteristics to quantitatively assess and detect anomalies in HVDC systems.

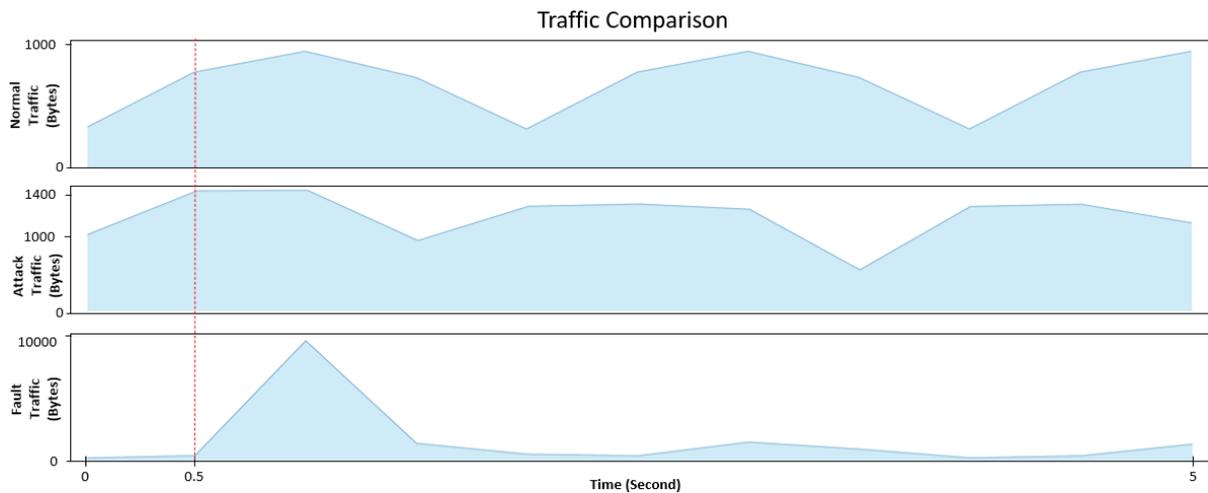


FIGURE 4-12: TRAFFIC COMPARISON FROM DIFFERENT SCENARIOS.

## 4.4. HVDC Cyber Attack Mitigation

### 4.4.1. State-of-the-Art Cyber Attack Mitigation on HVDC

State-of-the-art the research on defense against cyber threats can be classified into three groups, i.e., detection, mitigation and resiliency as seen in Table 4-4 applying to HVDC system. We classify and define the individual defense mechanisms as follows:

- 1) *Detection*: Identify the attack by differentiating it from the normal behavior of the network e.g.: Intrusion detection system, Anomaly detection, etc.
- 2) *Mitigation*: In case of a successful attack, taking actions or responding to minimize the effect of the attack on the system and operation e.g.: Incident response, Backup and recovery, security controls.
- 3) *Resiliency*: Taking suitable measures before an attack in order to cause minimum disruption and damage to the system e.g.: System hardening, zero trust, awareness training.

TABLE 4-4: SUMMARY OF CYBER DEFENSE METHODS IN HVDC POWER GRIDS.

REF.	DETECTION	MITIGATION	RESILIENCY
[75]	Threshold based	-	-
	Threshold based	-	-
[105]			
[88]	Threshold based	-	-
[108]	Threshold based	-	-
[100]	Threshold-based	-	-
[74]	Threshold based	Injecting control for firewall	-
[84]	Threshold based	Inject estimated measurement	-
[81]	Threshold based	Inject control to adjust power	-
[91]	Data Driven	Inject control to adjust power	-
[92]	Data Driven	Inject control to adjust power	-
[107]	Data driven	Inject control to adjust power	-
[93]	Data-driven	Inject estimated measurement	-
[89]	Data-driven, Model/Rule based	-	-
[99]	Model/Rule based	Inject control to adjust power	model communication with physical layer
[112]	-	Inject estimated measurement	-
[85]	-	-	model communication with physical layer

[86]	-	-	model communication with physical layer.
[103]	-	-	model communication with physical layer

## Detection

The state-of-the-art research considers the detection of cyber-attacks in an HVDC system using three techniques, i.e., threshold-based detection, data-driven detection, and model/rule-based detection. Two detection approaches to defend against spoofing attacks were proposed in [75]. The method calculates the expected AC side current of the HVDC system by using its AC side voltage and the AC voltage just outside the terminals. If the difference between the predicted and measured AC side currents is above a threshold, the attack can be detected. This method is shown to be capable of detecting the first two kinds of attacks. The combined DC voltage & power measurement attack can also be easily detected by calculating the DC current using the voltage difference across the DC terminal.

A mechanism for maintaining HVDC systems power order command security is proposed in [105]. The proposed method can detect inadvertent/insecure power order commands sent to the HVDC system at the right time and stop them from being executed while issuing an alarm. This method involves three stages as follows:

- The transmission lines' power flows resulting from a requested change in the power order command sent to the HVDC station are continuously estimated by using the concept of Power Transfer Distribution Factors (PTDF) [113].
- The possible effects of the received power order command are predicted based on the estimated transmission lines flows from the previous stage. The assessment considers threshold violations, voltage stability issues, harmonics, etc.
- If the requested change in the power order command is predicted to result in any unwanted security issues, its execution will be stopped, and an alarm will be issued to inform the HVDC station and the grid control center operators.

In [108], the authors identify the potential cyber-attacks on the measurements used by the HVDC control system. The proposed method uses the average model representation of HVDC systems to calculate error vectors for DC current and voltage measurements. The measured values from the DC current and voltage at the rectifier and inverter sides are then compared with calculated error vectors. If the difference is above a certain threshold, the existence of a cyber-attack can be detected. The simulation results presented in [108] show the effectiveness of the proposed approach in detecting the spoofing attacks on the HVDC system rectifier DC current and inverter DC voltage measurements.

A multifunctional control mechanism for HVDC systems was proposed in [100]. The proposed control mechanism enables the HVDC system to provide ancillary services such as frequency and voltage regulation and Fault Ride Through (FRT) capability. A framework that enables this control mechanism to distinguish between fault and cyber-attack conditions is also proposed in this report. When a short circuit fault appears in the system, different system variables (e.g., AC and DC side powers, voltages, and currents) change according to the Kirchoff's Voltage Law (KVL). On the contrary, when an attacker tries to modify one of these parameter values maliciously while neglecting its relations with other system parameters, the cyber-attack can be easily detected by using control approaches such as the ones proposed in [100]. The authors in [74] present a detection strategy using a predictive control-based approach. If the difference between predicted and measured active and reactive powers exceeds a pre-set threshold, the attack can be detected.

The authors in [91] propose a Squeeze-Excitation based double Convolution Neural Network (SE-DCNN) to defend against FDIA attacks on grid frequency of HVDC system. The proposed method is tested on different frequency FDIAs, including false oscillation attacks, scaling attacks, ramping attacks, playback attacks, and data interchange attacks. By running the simulations on a reduced model of the HVDC links between Spain and France considered in INELFE link, it is shown that the developed method performs well in identifying FDIAs of varying time durations, targeting the frequency measurement signal.

The authors of [91] continued their work on developing defensive mechanisms against frequency FDIAs on the HVDC systems in [92] by proposing a novel method that utilizes the Hilbert Huang Transform (HHT). HHT is used to decompose the system measurements into the Band-limited Mode Functions (BMFs) with Variational Mode Decomposition (VMD) algorithm. To automatically classify different types of frequency FDIAs on the HVDC systems (e.g., ramping attacks, scaling attacks, etc.), a Multikernel Support Vector Machine (MSVM) is also proposed. The K-means approach, which is a fast, unsupervised machine learning technique, is also used in the proposed defensive approach to calculate the attacks duration time.

The authors in [107] propose a cyber-attack detection framework using a special kind of artificial intelligence algorithm called Attack Shuffle convolutional neural Network (ASNet) which learns the intrinsic characteristics of cyber-attacks on HVDC systems. First, a Continuous Wavelet Transform (CWT) method is used to extract the time-frequency features of the input measurements. The results obtained from the CWT are then used as inputs to the ASNet to identify the type of cyber-attack. Continuous Wavelet transform and ASNet is used to detect the attacks quickly.

In [93], a Multi-Agent System (MAS) was proposed to detect and neutralize cyber-attacks targeting the AGC and HVDC systems. The attack detection is performed centrally by a master agent, while the attack mitigation is decentralized by slave agents installed at local HVDC stations and generating units. In order to detect the occurrence of a cyber-attack at the master agent, the Support Vector Data Description (SVDD) classifier (which is one of the most promising One-Class Classifier models) is utilized for anomaly detection as it can detect unseen events while being trained just using the secure normal data.

The authors in [89] state that HVDC applications typically rely on one or two-way communication links between the HVDC station and control center, nearby substations, and other control facilities. HVDC station configurations, including HVDC controller settings and parameters, are also usually transmitted to relevant control center applications for stability assessment purposes. These access points to HVDC stations increase the risk of potential cyber-attacks targeting their performance. HVDC systems can be used for different applications in power grids, i.e., Wide Area Damping Control (WADC). WADC is designed to reduce low-frequency inter-area oscillations by relying on the collected PMUs data through the Wide Area Measurement, Protection, and Control (WAMPAC) platform.

Two different approaches are proposed in [89] to detect the occurrence of FDIAs targeting WAMPAC-based HVDC applications. In the first approach, a learning-based model capable of classifying between normal and attacked grid conditions is built using Extreme Learning Machine (ELM) theory. The collected PMU measurements (including voltage, current, and power phasors) are used as inputs to this model. The second detection approach proposed in [89] is actually a model-based method that considers the correlations between physical measurements obtained from PMU data. PMU data in a power grid are linked together and follow physical laws and circuit equations, such as Ohm's law and Kirchhoff's laws (KVL and KCL). Therefore, each measurement value can be predicted using others in the grid. This predicted value can then be compared with the actual measured one. If there is a

considerable difference between these two quantities, the existence of an attack can be detected. The performance of the proposed detection methods by [89] is tested on a two-area system designed for analyzing HVDC systems WADC application. The authors in [99] detect the attack based on the timestamp and message hash code.

#### Mitigation

As for mitigation, the papers talk about injection control or estimated measurements in case the detection algorithm detects an attack. The authors in [74] mitigate the attack by enabling or disabling the firewall gate. A mitigation attack strategy by compensating the untrustworthy voltage with voltage estimated by the Kalman Filter estimate was proposed in [84].

The authors in [112] propose an optimal cyber defense strategy for HVDC systems to reduce the grid frequency deviations resulting from manipulated measurements. It is assumed that an attacker is trying to increase the frequency deviations in the grid by attacking an HVDC station controller. The attacker does so by injecting a positive (if the pre-attack frequency deviation of the grid is positive) or negative (if the pre-attack frequency deviation of the grid is negative) value to the station controller. After the defender (e.g., the grid operator) detects the occurrence of the attack, they try to find an optimal sequence of corrective injections into the HVDC station controller to oppose the attacker and restore the grid frequency to normal, acceptable ranges. This sequence of both cyber-attacks and defense strategies is viewed as a multi-stage decision-making problem in [112], which is then transformed into a single-level Mixed Integer Quadratic Programming (MIQP) problem. The simulation results presented in [112] show that the proposed defense strategy can effectively restrict the frequency deviations (by preventing the frequency deviations from going beyond the  $\pm 0.5$  Hz range) in the face of cyber-attacks on a two-terminal LCC HVDC system.

The authors in [91] developed Squeeze-Excitation Double Convolutional Neural Network (SE-DCNN) framework for defending against frequency FDIAs. This method is also used to propose an HVDC control approach that is capable of suppressing the frequency attack impacts on the integrated AC/DC power grid. In case of a cyber-attack being detected, the mitigation algorithm sends control commands to adjust the current power flow back to the scheduled power flow. In [92] a Hybrid Data Driven (HDD)-based control framework for the HVDC system is proposed to defend against the attack and reduce the impact of the attack on the performance of the ancillary services provided by the HVDC systems. The authors in [107] develop a Wide area power oscillation and damping control framework to mitigate the effects of cyber-attacks. Based on the type of attack identified by the detection algorithm, a suitable control strategy is activated which modifies the power output of integrated cyber-attack defense control and reanalyzes the Low frequency oscillation model. The authors in [99] mitigate the attack by injecting control sequences when an attack is detected. The papers use Single input single output controlled autoregressive and moving average models for predictive control.

The authors in [92] proposes a mitigation strategy using the slave agents to generate alternative control signals when notified by the master agent in case of an attack. The slave agents predict control signals using a data driven Support vector regression model. In [81], the authors proposed an event-triggered cyber defense strategy to mitigate the effects of rapid frequency deviations caused by non-simultaneous cyber-attacks on the multi-infeed HVDC system. The strategy involves coordinating compromised LCC HVDC systems and AC systems using a mixed-integer quadratic programming framework, which is solved online and updated when new cyber-attacks occur.

#### Resiliency

Some of the research discusses cyber resiliency strengthening against attacks by modeling communication layers and their effects on the physical system. In [99], a resilient wide-area damping control scheme for HVDC systems based on a Secure Networked Predictive Control (SNPC) mechanism was proposed. The paper models the cyber layer along with the physical layer to show the effects of deception attacks on the network. Along with deception attacks the paper also considers data modification, time delay, packet dropout, data replay, and data breach. The mechanism aims to ensure data confidentiality, integrity, and authenticity. The authors in [85] and [86] investigated the importance of modeling the cyber-related components involved in the control system of MMC-HVDC systems for analyzing their stability margins. Specifically, the effects of measurement sampling and data processing delays, signal transmission delays, and PWM modulation procedure delays are incorporated into the state space model of the MMC-HVDC system. Then, two approaches based on approximation [85] and Rekasius substitution [86] are proposed to derive the stability margins of the system. Based on the simulation on a multi-terminal VSC-HVDC system, this research proved that the mentioned cyber delays could result in system instabilities and induce sub-synchronous oscillations (around 35 Hz) in the system variables. The findings of [85] and [86] are also interesting from the cyber security point of view, as the attackers can create stability issues in the system by conducting time delay attacks on the measurements used by the HVDC control system. The authors in [103] consider the communication failures in the wide-area control for inter-area oscillations. They propose a dynamic heuristic-based wide-area damping control mechanism to dampen inter-area oscillations in a Voltage source converter-based HVDC system. The model is able to perform damping control under one and two-channel communication failure without needing an accurate model of the physical layer.

#### Summary of State-of-the-Art Research on HVDC Cyber Security

According to the systematic literature review, the state-of-the-art cyber security research on HVDC systems can be summarized into the following conclusion points:

- The current cyber security research on HVDC only considers the later stage of the cyber kill chain after the adversaries successfully compromise the system, i.e., FDIA, replay attack, and DoS. The early phase of cyber kill chain has not been included in the state-of-the-art studies. Therefore, most of the research is only based on the prior assumption that the HVDC cyber-attacks already reach and compromise OT system.
- The state-of-the-art cyber defense for HVDC system primarily focused on the detection using threshold base, data-driven, and rule-based. For the mitigation, the research uses control injection for power adjustment. Meanwhile, some research proposes resiliency improvement through HVDC modelling and simulation. Based on the current trends, the mitigation only focuses on power system aspects and omits cyber mitigation.
- The current research heavily focused on the modelling of the HVDC physical systems and did not incorporate the cyber element. Although the research aims to provide a solution for the cyber-attack on the HVDC, only the physical element is considered and use the cyber-attack is based on assumptions.

#### 4.4.2. Deep Learning for Throughput Anomaly Detection

Cyber-attack in power grids may employ several attack strategies and steps to achieve their objectives. These can be mapped with the seven stages of the cyber kill chain for an in-depth analysis of such an advanced persistent threat, i.e., reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action on objectives as depicted in Figure 4-13. The state-of-the-art cyber

security on HVDC system is mainly focused on power system anomalies that occur when an attack is successfully executed at the later stages of the cyber kill chain, e.g. FDIA. In contrast, in the real cyber-attacks of Ukrainian power grids in 2015 [109], the cyber kill chain lasted for more than six months between the reconnaissance and command and control stages. Hence, this highlights the urgency of timely early-stage attack detection through Information Technology-Operational Technology (IT-OT) system anomalies. Physical measurement-based anomaly detection is only valid for later stages in the cyber kill chain, i.e., command and control and actions on objectives. Therefore, in this report, we implement an early-stage anomaly detection method for OT systems. It is possibly to be implemented in the control center to detect cyber-attacks at the early stages of the cyber kill chain, based on throughput anomalies in OT communication traffic. The following part describes the methods for anomaly detection in OT network, i.e., traffic pre-processing dispersion graph and attack graph model.

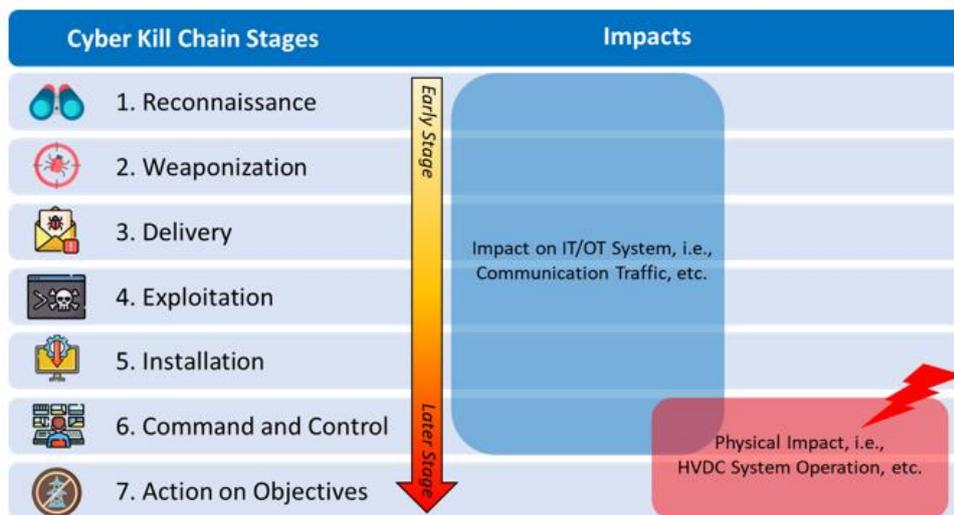


FIGURE 4-13: CYBER KILL CHAIN STAGES AND IMPACTS.

### Traffic Preprocessing Dispersion Graph

The IT and OT network traffic characteristics exhibit notable distinctions. The network traffic in OT systems originates from automated processes with deterministic and homogeneous behavior [114]. In contrast, the traffic in IT systems primarily comprises user-generated data that has a stochastic behavior. Therefore, the implementation of traffic-based anomaly detection for OT systems fundamentally differs from that of IT systems.

Communication network forensics involves the process of collecting, preserving, and analyzing network data in order to detect and investigate unauthorized access [115]. It is a crucial component of network security, as it enables organizations to quickly detect and respond to cyber threats. Network administrators typically employ network traffic analysis tools to perform network traffic forensics, which involves capturing and analyzing traffic data in real-time or from historical traffic logs. These tools aid in detecting network anomalies, such as abnormal traffic patterns or unauthorized access attempts, that may suggest security breaches or malware infections. Wireshark, Tshark, Snort, and tcpdump are well-known software tools for network traffic analysis. These tools can capture network traffic data and provide a comprehensive analysis of the data, including the source and destination of the traffic, traffic type, and any detected anomalies or suspicious activities.

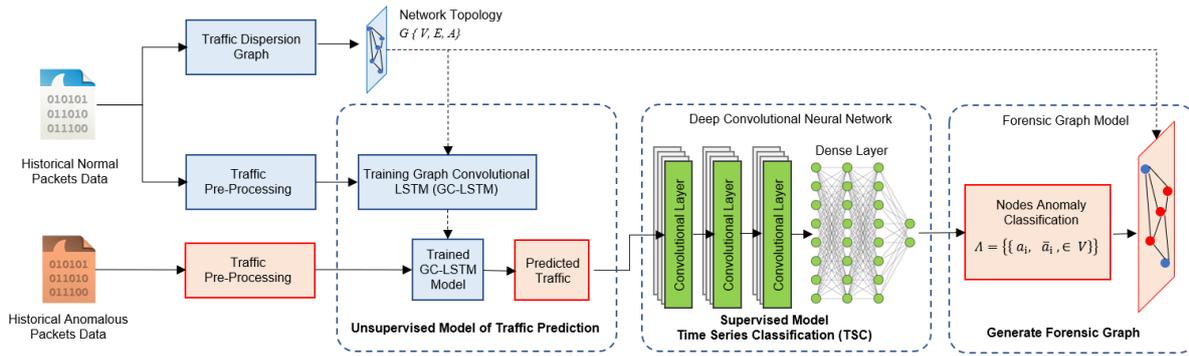


FIGURE 4-14: FORENSIC GRAPH MODEL FOR ANOMALY DETECTION.

One of the methods to perform a deep forensic analysis is through network forensic data visualization [116]. A matrix-based visualization from network forensic data was presented in [117]. The authors show the visualization summary of network data, e.g., IP addresses, ports, NetFlow payloads, entropy of source and destination IP, etc. The visualizations help to facilitate network traffic analysis and pinpoint anomalies within the network. An alternative method to visualize the network traffic data is using a Traffic Dispersion Graph (TDG). The TDG is an analytical framework utilized for the purpose of observing and evaluating communication traffic. The fundamental concept behind TDG is interactions between hosts within a network [118]. Moreover, TDG employs graph structures to represent nodal information. Each individual node in a graph represents an individual host within a network. Conversely, the transmission of information among hosts is denoted by the interconnectivity of nodes, i.e., graph edges. Previously, the TDG was utilized to analyze communication network patterns. For instance, studies in [119] proposed an application of TDG for anomaly detection, based on graph information from network traffic. As shown in Figure 4-14, we use TDG to generate a network graph topological representation from recorded OT traffic data.

Besides the aforementioned TDG, we also implement Traffic Pre-Processing (TPP) in the model for the historical packets. This extracts information from the packets, i.e., nodes, edges, and time series traffic throughput. Algorithm 5.1 summarizes the pseudocode of both TDG and TPP. The input for the proposed algorithm is historical traffic packets ( $P$ ) captured using Wireshark or Tshark. TDG processes the OT traffic to extract Graph information ( $G$ ) from the packets, including vertices/nodes ( $V$ ), single node ( $v$ ), group of edges ( $E$ ), single edge ( $e$ ), and the adjacency matrix ( $A$ ). Meanwhile, TPP aims to convert the packets into time series throughput data for each node ( $X$ ). The extracted graph ( $G$ ) and time series throughput ( $X$ ) serve as input for the subsequent forensic graph stages.

---

**Algorithm 5.1: TDG and TPP Algorithm**

---

**Inputs:**  $P$ : Historical communication traffic packets

**Outputs:**  $G = \{ \{ V, E, A \} \}$ : Graph with nodes, edges and adjacency  
 $\{ x_1, x_2, \dots, x_v \}^t \in X$ : Time series throughput data

---

- 1 TDG iteration for each packet  $p$  in  $P$   
**for**  $p$  in  $P$  **do**
  - 2     **if**  $v$  **not in**  $G\{V\}$
  - 3         add  $v$  to  $V$
  - 4     **if**  $e$  **not in**  $G\{E\}$
-

```

5           add e to E
6       end for

7   TPP throughput extraction iteration for each time t in T
   for t in T do
8       for v in G{V}
9            $x_v^t = \sum x_v$ 
10      end for
11  end for
12  return G = {{ V, E, A }} and {x1, x2, ..., xv}t ∈ X

```

---

### Graph Convolutional Long Short-Term Memory

Graph Convolutional Long Short-Term Memory (GC- LSTM) is adopted to acquire knowledge about the OT network traffic patterns. GC-LSTM employs two machine learning models, i.e., Graph Convolutional Network (GCN) and LSTM. The GCN utilizes graph-based representations of the OT network's topological information, in conjunction with localized features derived from neighboring communication nodes in the spatial domain. Subsequently, LSTM is employed for temporal learning by utilizing time-series data of observed OT network traffic. The integration of GCN and LSTM confers the benefit of acquiring knowledge from both, the spatial and temporal domains.

The primary input for the GC-LSTM approach is the graph structure of the OT network topology. TDG is used to derive this particular graph structure, as previously described. The Graph (G) elements are vertices/nodes (V), edges/links (E), and adjacency matrix (A). The adjacency matrix is a representation of elements denoted by  $A_{i,j}$ , where  $i$  and  $j$  are node index numbers.  $A_{i,j}$  equals 1 when two nodes are connected and 0 when they are not.

In Eq. 4.1, the GCN model is predicated on the Hadamard product multiplication ( $\bullet$ ) of the weight matrix ( $W_{gcn}$ ), adjacency matrix (A), and node features derived from the historical traffic data ( $X_t$ ). The adjacency matrix is a mathematical representation that encapsulates pertinent details concerning the topology of the OT network. The modified adjacency matrix ( $\hat{A}$ ) is obtained by adding the identity matrix (I) to the original adjacency matrix (A). The time series data set ( $X_t$ ) is modelled by an equation that accounts for a specific time point ( $t$ ) and the overall number of time observations ( $T$ ). The node feature matrix (X) contains information about each node ( $x_i$ ), where n represents the total number of nodes. The equation takes into account the exponent  $k$ , which represents the number of hops from a communication node to its neighboring nodes, as described in [120] and [121]. Following the acquisition of spatial features through the GCN, the LSTM model is subsequently employed to examine the temporal or time-series characteristics. The functions and processes that occur within an LSTM cell are described in Eq. 4.2–4.7. The LSTM process comprises six primary sub-equations, namely the sigmoid function ( $\sigma$ ), forget gate ( $f_t$ ), input gate ( $i_t$ ), output gate ( $o_t$ ), internal cell state ( $c_t$ ), transferable cell state ( $c_t$ ), and hidden state ( $h_t$ ).

$$GCN_t^k \leftarrow (W_{gcn} \bullet \hat{A}^k) X_t \quad (4.1)$$

$$f_t = \sigma((W_f GCN_t^k) + (U_f h_{t-1}) + b_f) \quad (4.2)$$

$$i_t = \sigma((W_i GCN_t^k) + (U_i h_{t-1}) + b_i) \quad (4.3)$$

$$o_t = \sigma((W_o GCN_t^k) + (U_o h_{t-1}) + b_o) \quad (4.4)$$

$$c_t' = \tanh((W_c GCN_t^k) + (U_c h_{t-1}) + b_{c'}) \quad (4.5)$$

$$c_t = (f_t \bullet c_{t-1}) + (i_t \bullet c_t') \quad (4.6)$$

$$h_t = o_t \bullet \tanh(c_t) \quad (4.7)$$

### Time Series Classification and Forensic Graph Model

Time Series Classification (TSC) was implemented in [122] for anomaly detection. In this report, we present a method for detecting anomalies in OT communication network traffic using TSC. The method employs a hybrid approach that combines both supervised and unsupervised methods for detecting anomalies in OT traffic. The utilization of unsupervised learning for time series data was implemented in [88]. Hence, an unsupervised Graph Convolutional Long Short-Term Memory (GC-LSTM) model is employed to acquire knowledge of the intricate patterns exhibited by OT network data and topology. Following this, the GC-LSTM model produces traffic predictions which serve as inputs for the TSCs.

$$y_i^l = \text{ReLU}(\sum_{(i)}^{m-1} w y_{(i)}^{l-1} + b) \quad (4.8)$$

$$F_G = \{\{f_i, \bar{f}_i, \in V\}\} \quad (4.9)$$

TSC is implemented using a CNN algorithm with a multi-layer convolutional and ReLU activation function, as described by (4.8). The variables under consideration in Eq. 4.8 are the number of layers (l), filter size (m), weight (w), and bias (b). The CNN algorithm performs binary classification of each node as normal or anomalous. The classification is performed based on TSC from time series throughput data for each node (X). The result from the classification is then used to construct a forensic graph in the following stages.

The forensic graph equation is described in Eq. 4.9. The FGraph is constructed based on prior knowledge regarding the topology of the OT network as well as the results of the node classifications. The FGraph ( $F_G$ ) comprises two distinct components, i.e., normal nodes ( $f_i$ ) and anomalous nodes ( $\bar{f}_i$ ). The node classifications, alongside the graph structural information, are then used to visualize the FGraph with different node colors. The node color variations help the user to pinpoint anomalous locations within the OT network topology.

#### 4.4.3. Forensic Graph Model for Anomaly Localization

A forensic graph is a method to model CPS vulnerabilities and potential exploits. Since a successful exploit of a vulnerability may lead to a partial or even a total failure of the CPS, a forensic graph is an important tool for vulnerability analysis and mitigation strategies. Meanwhile, in a communication network, there are many hosts that may become vulnerable. As a result, the cyber security of the entire CPS cannot only rely on the security of a single host. Therefore, it is important to locate and

identify all vulnerable nodes/hosts in a communication network as a set of potential threats in the CPS. The observation and analysis of anomalous OT traffic behavior to detect nodes potentially compromised by cyber-attacks is implemented using the forensic graph. The information regarding anomalous nodes is then used to construct a forensic graph for the OT network of the power grid.

For evaluating the performance of the FGraph, we collect data from the experiment setup summarized in Table 4-5 which represent HVDC OT communication traffic. Other than the aforementioned experimental set up, in this sub-section, we also analyze multiple open datasets, i.e., IEC 61850 [123] and DAPT 2020 [124]. In [123], the authors provide communication data from a digital substation based on IEC 61850 standard. The dataset provides OT communication traffic data under normal, disturbance, and cyber-attack scenarios. Normal data is derived from normal traffic with and without variable loading. The disturbance scenarios include busbar protection, breaker failure protection, and Under Frequency Load-Shedding (UFLS). The cyber-attack scenarios cover Denial of Service, GOOSE spoofing, merging unit measurement spoofing, circuit breaker Boolean value injection, and replay attack.

In [124], the authors generate data based on normal and Advance Persistent Threat (APT) traffic for a duration of 5 days. The scenarios implement various stages of cyber-attack kill chain, including vulnerability scanning, exploitation, establishing a foothold, privilege escalation, etc. The experiments incorporate red team and blue team tools, e.g., Metasploit and Snort. The NetFlow data collected from the experiment within 5 days includes source, destination, flow duration, flow bytes, etc. However, the provided NetFlow CSV data is not suitable for our proposed method of TDG and TCC. Therefore, in this subsection, we use the provided raw original source of packet data in .pcap format.

**TABLE 4-5: SUMMARY OF NETWORK TRAFFIC DATA.**

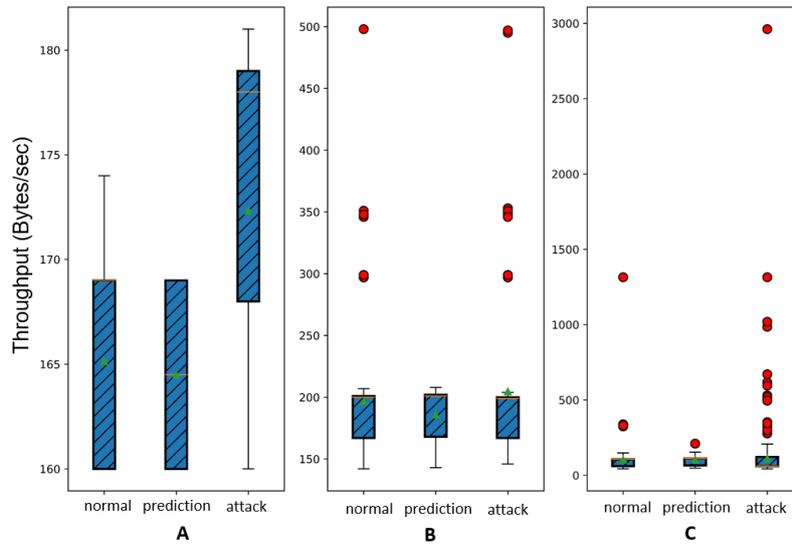
PARAMETERS	A	B	C
NO OF NODES	85	103	786
NO OF EDGES	198	246	821
TRAFFIC DURATION	30 minutes	150 minutes	5 days
TOTAL PACKET SIZE	50 MB	100 MB	17 GB

Table 4.5 summarizes the network traffic data from the experimental HIL (A), IEC 61850 dataset (B) [123], and APT dataset (C) [124]. Data A and B originate from the substation models within a local network, which primarily transmits layer 2 broadcast messages using MAC addresses. Meanwhile, data C is dominated by layer 3 communication using IP addresses. Data C also indicates that the network is segregated into private and public networks. Additionally, this data has the most accumulated packet history of 5 days, with a total size of 17 GB.

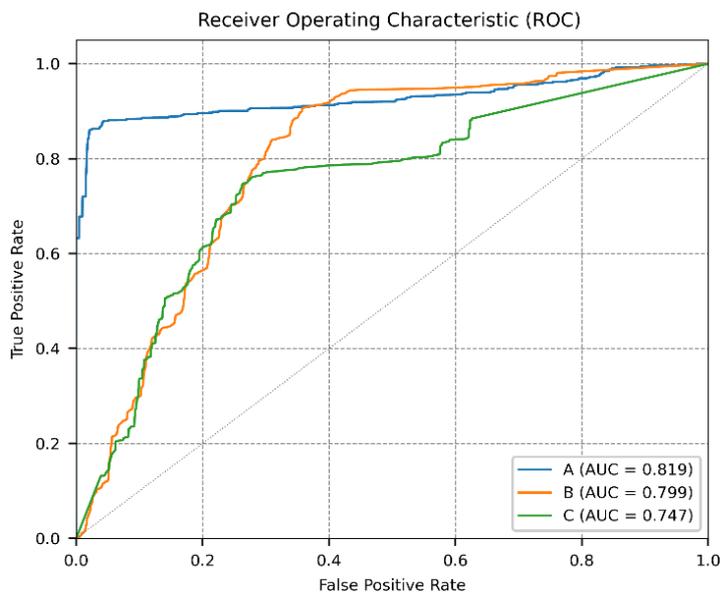
All the aforementioned data is then processed using the forensic graph generation model. The GC-LSTM generates traffic predictions that serve as a normalization filter. Figure 4-15 depicts a statistical comparison as box plots between normal, predicted, and attack traffic for all 3 cases. As shown in Figure 4.16, normal traffic also contains outliers, indicated by red dots. These outliers can affect classification performance and result in increased false positives. Meanwhile, in the predicted traffic, the outliers are significantly reduced. Therefore, GC-LSTM helps to improve the classification accuracy of the CNN time series classifier.

The anomaly detection is performed based on TSC using CNN. TSC classifies the traffic throughput as normal or anomalous. Figure 4-16 shows the performance comparison for each dataset using the Receiver Operating Characteristic (ROC) curve. Dataset A provides the best result with an Area Under

the Curve (AUC) score of 0.819, followed by datasets B and C. Results for dataset C show the worst performance as the data contains more noise compared to the other two datasets.

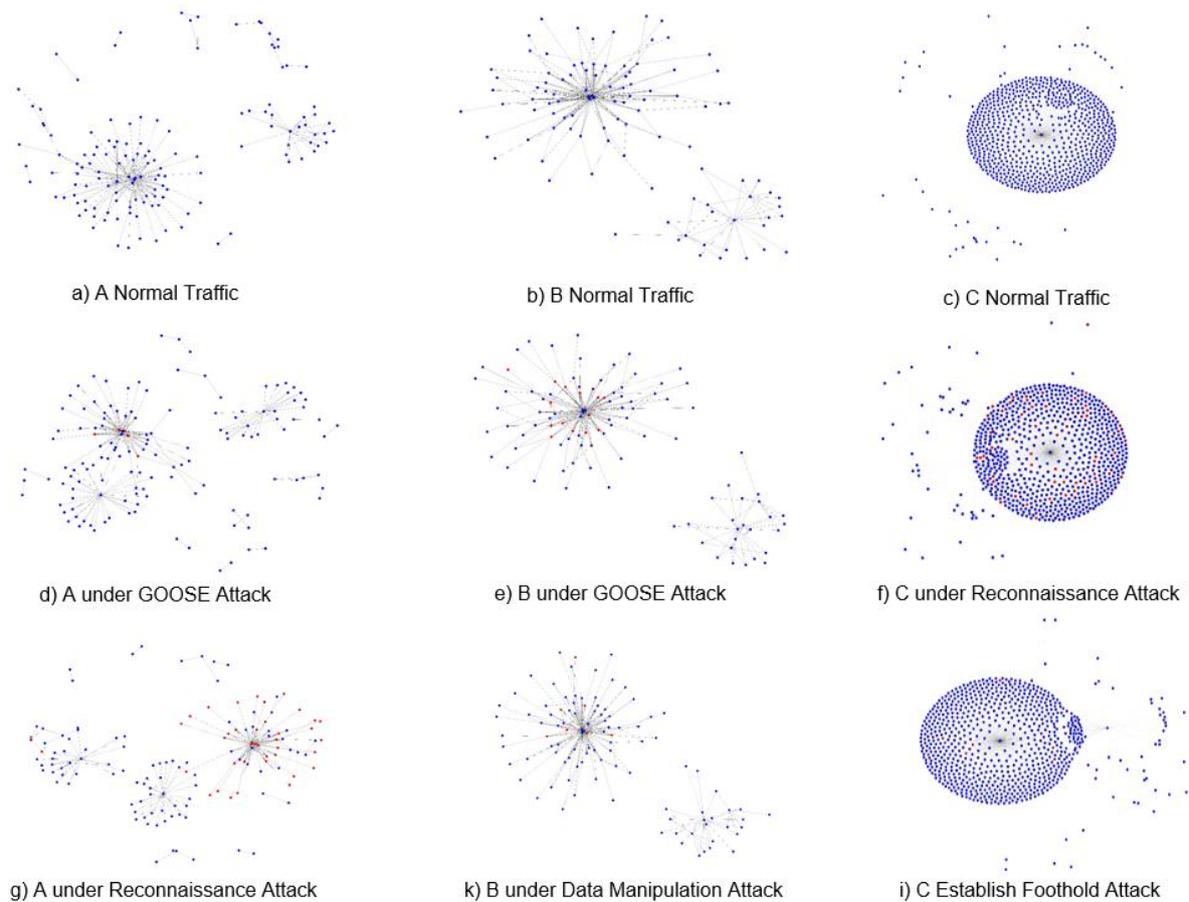


**FIGURE 4-15: STATISTICAL COMPARISON BETWEEN NORMAL, PREDICTED, AND ATTACK OR ANOMALOUS TRAFFIC FOR DATA A, B, AND C.**



**FIGURE 4-16: ROC COMPARISON FOR DATA A, B, AND C.**

Figure 4-17 shows the forensic graph plot for normal and anomalous traffic. The blue node represents normal traffic, while the red one represents anomalous traffic. Figure 4-17 a, b, and c show the graph representation from normal traffic, while the others show the graph under attack scenarios. The cyber-attack scenarios include GOOSE replay attack, reconnaissance, data manipulation, and foothold establishment. The graph comprises nodes that store data pertaining to the source and destination IP addresses or MAC addresses, as outlined in the TDG references [125], [118], and [119]. Results from the TDG show the ability to identify anomalous nodes within the network by tracing them back to their respective IP or MAC address. The operator utilizes these particular IP or MAC addresses to identify the root causes of the traffic anomaly. These IP and MAC addresses can potentially be associated with a compromised host or a host that has been targeted by an attack.



**FIGURE 4-17: FORENSIC GRAPH MODEL PLOTS.**

#### 4.4.4. Implementation of Secure Standard Protocol

This sub-section presents a spoofing attack that specifically targets and manipulates GOOSE traffic within the digital substations of HVDC grids. This showcases the exploitation of vulnerabilities in the GOOSE protocol utilized by protective relays. The spoofing attack caused the unintended opening of the breaker in the HVDC grids, resulting in abnormal behavior of the HVDC system. A viable measure to prevent spoofing attacks entails assuring the authenticity and integrity of the message by employing authentication codes at the end of every GOOSE message, as specified in the IEC 62351-6 standard.

The security of the protocols specified by IEC 61850 is addressed by the IEC 62351-6 standard. The proposal suggests adding a new category to the GOOSE and SV data payloads Protocol Data Unit (PDU) specifically for security-related information. The PDU is secured with a Rivest-Shamir-Adleman (RSA) based signature, which guarantees its integrity. This measure allows the IED message sender verification and avoids GOOSE message manipulation. However, the recommended implementation of RSA signatures to ensure message authenticity and integrity renders it inappropriate for use in scenarios that require a maximum response time of 4 milliseconds [126]. The reason for this is that RSA encryption and decryption require significant computational time. In addition, the standard does not include any details regarding the certificates associated with the RSA keys utilized for signing extended PDUs. Moreover, the utilization of RSA-based authentication keys for IEDs implies the implementation of a key management infrastructure within the digital substation. RSA and Elliptic Curve Digital Signature Algorithm (ECDSA) performance for GOOSE message security were evaluated

in [127]. However, neither of them can meet the time requirement. Due to these factors, the utilization of GOOSE security mechanisms has not yet become prevalent.

**TABLE 4.6: PERFORMANCE OF MESSAGE AUTHENTICATION CODE**

ALGORITHM	COMPUTATIONAL TIME (MICROSECOND)	LATENCY (MICROSECOND)	
		Average	Max
HMAC-SHA-256	14.3	75.7	78.0
AES-GMAC-64	6.6	73.0	75.3
AES-GMAC-128	7.0	74.9	77.1

To address the limitations of the digital signature, the authors in [128] studied the application of Message Authentication Codes (MAC). According to the experimental results, the computational times of MAC algorithms are considerably faster than RSA and ECDSA. Table 4.6 shows the comparison performances of MAC variations. Implementing MAC could potentially serve as an alternative solution to enhance the security of the IEC 61850 standards while maintaining the necessary time requirements. In order to enhance the security of HVDC grids against potential cyber-attacks, it is essential to implement a protocol security standard in conjunction with an anomaly-based mitigation strategy.

## 5. General Conclusions

Task 3.3 aims to provide comprehensive guidelines for the cost-effective design of HVDC-based grid architectures capable of withstanding faults occurring on the DC side, AC side, or within the cyber layer. Through the implementation of three subtasks, significant progress has been achieved towards achieving this overarching objective.

In chapter 2, the Subtask 3.3.1 focus has been on devising cost-effective AC/DC systems resilient to DC faults, emphasizing the broader impact on the entire transmission network. By utilizing EMT simulations and analyzing various grid scenarios, including factors like AC grid strength and converter control modes, valuable insights have been gained into the impact of well-known DC protection sequences on AC grid stability. Future efforts will concentrate on developing dedicated HVDC control strategies to mitigate these impacts effectively.

In chapter 3, Subtask 3.3.2 is dedicated to examining the implications of AC protection in converter-dominant regions. Through a systematic analysis of fault scenarios and line characteristics, the task aims to determine the necessity of adapting existing AC protection schemes. The forthcoming guidelines will offer insights into AC protection philosophies coordinated with diverse control strategies.

In chapter 4, Subtask 3.3.3 delves into the cyber vulnerabilities of HVDC systems and assesses the potential impacts of cyber-attacks on grid performance. By exploring communication-related aspects in the context of cyber-resiliency, the task sets the stage for identifying vulnerabilities and proposing defensive mechanisms against cyber threats. Future endeavors will focus on uncovering vulnerabilities and impacts of cyber-attacks on HVDC-HVAC systems, facilitating the development of robust anomaly detection strategies based on power system measurement data and operational technology traffic.

Overall, the progress made in Task 3.3 lays a solid foundation for the development of guidelines crucial for ensuring the resilience and reliability of HVDC-based grid architectures in the face of various fault scenarios, thus contributing to the advancement of future energy systems. Next subsections introduced the detailed conclusions of each subtask, providing the recommendations for the next working packages.

### 5.1. DC FRT Analysis Conclusions

The DC FRT operation of HVDC systems approaching MTDC grids has been analyzed in chapter 2, where different grid characteristics, control strategies, converter configurations towards performance standards have been considered. The main objective of this chapter is to evaluate the impact of the DC protection philosophies regarding R&R, therefore the characterization of the DC FRT for different control strategies is carried out and the proposition of new solutions to ensure the stable operation of system when impacted by DC fault are developed. The analysis also encompasses frequency dynamics involving synchronous machines and PE grids. This aspect aims to ascertain the effects of DC faults on the AC side of the grid and the potential interaction between frequency and voltage dynamics. It seeks to investigate the repercussions of DC faults and the propagation of disturbances between DC and AC systems, both in terms of their impacts and the propagation of perturbations.

Based on the analysis been done in this chapter, the DC FRT can be directed through some guidelines to reduce the impact of DC faults in the AC grid side, improving the security of the DC FRT and enhancing the stability in the AC side, resulting to improvements to reliability and resilience. As

extreme cases, fully selective and non-selective protection strategies have been assessed and the results used to define the approach taken as part of the study:

- A fully selective (FS) protection strategy has been designed to ensure continuous operation (non-stop operation), allowing the grid converter to remain in normal operation without interruption. This strategy involves a rapid response time for the DC breaker, typically between 3-5 ms, and DC reactors (DCR) are appropriately sized to mitigate fault currents. By delaying the triggering of the MMCs' blocking, the DC breaker is activated before the converter is affected. Consequently, fully selective protection minimizes the impact of DC faults, resulting in only negligible disturbances in the AC grid. This holds true even when employing GFM and GFL control strategies.
- The non-selective (NS) protection strategy encompasses a single protection zone covering the entire MTDC grid, rendering it highly susceptible to the impacts of DC faults. Under NS strategies, fault occurrences lead to the blocking of affected converters, necessitating subsequent restoration procedures once the fault is cleared. Consequently, power flow undergoes significant alterations during fault ride-through operations, warranting in-depth studies on grid stability and security. The NS strategy might cause the largest impact on AC stability when compared with FS and partially selective strategies. The initial step involves establishing the characterization of DC FRT with converters operating under GFL control. Subsequently, a detailed investigation into DC FRT characterization with converters operating under GFM control ensues, considering various AC grid configurations ranging from strong grids to low inertia weak grids such as PE grids.

#### 5.1.1. Characterization of DC-FRT

Considering NS protection, the characterization of the DC FRT in a MTDC grid with the converters operating in GFL control connected to a strong grid result with the expected power profile in DC FRT operation mode (a power peak at the moment of the fault, then going to zero power production after the DCCB is opened then followed by a linear power increase after the power operation is restored) of the stations affected by the DC fault (faulty poles). On the other hand, the converters not affected by the fault (healthy poles) remain in normal operation. In this context, the DC FRT starts with the DC fault inception, leading at first to the blocking of the faulty converters, followed by the opening of the DC breakers affected by the fault. Once the fault is isolated, the converters are allowed to be deblocked. The next step is to clear the DC fault by opening the switches in the MTDC, isolating the faulty cable. Once the converters are deblocked, the restoration of reactive power is possible, where the STATCOM operation of the converter is now available. From this point, the DCCB can be reclosed with no issues, creating a new MTDC configuration, since the faulty cables are now isolated. The next step is to reclose the DCCB, reconnecting the DC side of the grid, allowing the DC voltage restoration and then the active power restoration, thereby completing the fault restoration process. The temporary stop in this context is 400 ms.

When the SCR level is strongly reduced in the AC grid, composing a weak grid, the impacts of the DC fault are more relevant, where the AC voltage present deeper oscillations, and the power flow change caused by the fault can cause an unstable operation when near to the operational limits of the converter stations, mainly related to frequency stability. Therefore, the GFM control strategy arrives as a powerful solution to improve the operation of HVDC system in weak grid context. In this case, it might be necessary to adjust the inner current loop and PLL bandwidth to assure proper operation of the GFM control.

Once, GFM control is established, the characterization of the DC FRT when the converter is detailed developed in this chapter, by first extending the time scale of the protection sequence from 400 ms to 2.3 s, so the behavior of each stage of the FRT is described and analyzed. The first main feature of the GFM control is the reaction of the healthy pole to the DC fault when in bipolar configuration. In this case, the healthy pole provides AC grid support by injecting the power such that, the power imbalance caused by the fault is minimized, which represents the inertial response of the virtual machine to improve the frequency stability of the system. At the same time, the slower time scale dynamics are highlighted by the longer fault transients requiring the extension of the protection sequence duration. The perturbation of the faulty converter is reflected also in the healthy converter, just like any disturbance in the AC network also impacts the converters thanks to the GFM control characteristics. In addition, when the faulty converters are blocked, the virtual swing equation in the GFM converters are disabled, where the power reference is set to zero for safety reasons. It is necessary to reset the VSM controllers when the converters are deblocked. The reset values are given by the PLL measurement of frequency and phase angle of the connection point of the converter to minimize power peaks in the MMC, providing a smoother restoration process to the DC FRT operation.

### 5.1.2. Recommendations for DC-FRT in GFM converters

The extended protection sequence for the GFM control also highlights the internal energy problem when the converter is deblocked, after the DCCB is opened. During this period, the internal energy of the converter is not controlled since the DC side of the grid is in charge of controlling the capacitors submodules energy. Therefore, the internal energy is prompt to oscillations and instability after the converter is deblocked and the DC side is not available yet, since the GFM control can request power to control the AC voltage on the PCC, where the converter needs to provide reactive power, or even active power depending on frequency disturbances on the AC grid, harming the balance of the internal energy. Once the DCCB is reclosed, the internal energy is balanced again by the regulation of the DC voltage of the MTDC, in which the control is shared by the other converter stations. Thus, three different solutions are proposed to solve this problem:

1. Delay the deblocking of the faulty converter until the DC grid is reconnected, i. e. wait for the reclosing of the DC breaker, so the DC voltage on the faulty converter is again stable. In this case, the DC voltage on the faulty converter is not controlled, in between the deblocking of the converter and the reclosing of the DCCB, once the DCCB is reclosed, the DC voltage is handled by the other stations controlled in Vdc mode. The delays on deblocking the faulty converter is the simplest approach, not requiring any update in the hardware or in the control layer of the MMC, but only affecting the protection sequence. The disadvantage of this option is that the converter is not able to perform reactive power support, by operating in STATCOM mode, which can be crucial for the system operation in weak grids.
2. Shift from GFM to GFL control during the DC FRT operation. To avoid the internal energy instability issue, and the oscillations and slower transients identified in the characterization of the DC FRT operation in GFM control, it is possible to switch from GFM to GFL control when the converter is deblocked, where the flag to shift the operation mode to GFL is identified by the deblocking of the converter. It means that the converter is going to always initiate the restoration process in GFL control mode. This option can be very beneficial to reduce overshoots caused by the GFM feature and its slower dynamics, so GFL mode is able to perform the faster protection sequence with less impacts and smoother restoration. The GFM mode is reactivated once the DCCB is reclosed and the DC voltage control is reestablished, therefore, the active power restoration is done taking into account the inertial response of the VSM dynamics. In this case, the reactive power support with the STATCOM mode is not

affected during the DC FRT operation. The healthy converter remains in GFM control mode during the whole DC FRT operation, keeping the AC grid support.

3. Insert an outer control loop of the internal energy to be controlled by the active power on the AC side of the grid. In this case, during the time in between the converter deblocking and the reclosing of the DCCB, the internal energy is controlled by the AC side of the grid, since the DC side is not available, solving the stability issue of internal energy and maintaining the GFM control model during the whole process of the DC FRT. The outer loop is inserted as a power reference summed with the power reference in the VSM power control loop (e. g. added as power input in the virtual swing equation, since the actual power reference during this period set to zero when the converter is blocked). The outer control loop is designed according to the time dynamics of the VSM control, where the time constant of the internal energy becomes much slower during this stage to respect the time constant ( $T_s = 2s$ ) of the GFM power control. The outer energy loop is deactivated once the DCCB is reclosed, not affecting the power reference in the swing equation during normal operation. The great advantage of this option is the possibility of keeping the GFM characteristics of the GFM control during the whole process, where any other action is needed to perform the DC FRT operation. The disadvantage is to have a very slow time dynamic to the internal energy during the period where the AC power is controlling it.

### 5.1.3. Current limitation issues

When considering the DC FRT operation of HVDC stations, the operational limits of the converter represent an important constraint for the system behavior and stability, since when the converter is close to the nominal capacity, the current limitation algorithms can be activated to protect the converter to operate inside the safe operating levels. This safe operation is mainly related to the maximum allowed current in the converter (IGBT limits), such that the equipment is not damaged. This value is usually 1.2 pu of current magnitude for power converters, highlighting the limited overload capacity of power electronics equipment (20% overload capacity maximum). The current limitation behavior is evident concerning the support to AC grid (ancillary services) when the converter headroom is close to limits, in which the support to transients becomes very poor. This limits significantly the contribution of power converters to large signal stability when compared with synchronous machines. Two different current limitation algorithms are analyzed in this study, and the characteristic of each option is described next:

1. The Current Saturation Algorithm (CSA) saturate the current in a certain limit during transients, where the active power can have the preference, limiting the d component of the current in the given limit, and the q component limit is given by the complement to the maximum value. The other way around is also a possibility, providing the limits to reactive power supply. This approach is suitable for GFL operation, being inserted in the current control loop straightforward application. When the converter is in GFM control, an inner current control loop must be created in order to apply the CSA algorithm to limit the current in the GFM strategy. This control loop is created by inserting an inverse current control loop using the controlled voltages and the measured current in the converter. The current loop is only activated during current limitation operation [30]. During the current limitation operation, the system behaves as a current source, not being able to control the voltage in the GFM control mode. Therefore, synchronization problems and even instability issues can appear in critical conditions.
2. The Virtual Impedance (VI) algorithm consists of inserting the effect an impedance when the current exceeds the maximum allowed value, by introducing a virtual voltage drop

referred to voltage control loop of the converter. In this case, the voltage behaviour of the GFM control mode is preserved, but it is not suitable for GFL mode. The advantages of this algorithm are related to the improvement the transient stability of the system, nevertheless it can present overshoots during the initial current transients, which is not desirable for current saturation purposes.

#### 5.1.4. Influence of frequency dynamics in DC faults

The frequency dynamics of the AC grid is considered by including synchronous machines models and their related control blocks (AVR+PSS). The interaction between the GFM converters and the grid is much more pronounced, since the perturbations in the AC system are shared by the converters in GFM control. Therefore, frequency variations and changes in the operating point of the system can affect the control performance of this system. Therefore, the DC FRT operation is also impacted by the frequency dynamics of the AC grid, which can be critical when the DC side of the grid is not available for the converter (DC FRT stage where the converter is deblocked, but the DCCB is still opened). In this case, the frequency variations in the AC grid (RoCoF issues) will cause a reaction of the VSM swing equation asking for a power response from this converter, interfering in protection sequence operation. Therefore, the outer energy control loop can be very useful to maintain the balance in the internal energy and DC voltage on the converter, when VSM control reacts to an AC grid perturbation. In this case, the VSM response from the AC grid perturbation creates a power response that uses the active power to respond to that perturbation also considering the internal energy balance, so the DC side power is not really needed. A point of attention is critical referring to the speed dynamics of the outer energy loop, since the time constant is very slow when compared with the controller given by the DC side of the grid, the energy control is limited to the time constant of the VSM control. Therefore, if the perturbation requires fast reaction to bring balance to the grid, the outer loop controller is limited to a slow response.

When considering frequency dynamics, the local RoCoF can be considered an index to evaluate the impact of the DC fault in the surrounding synchronous machines connected to the MTDC link. In this case, the DC fault will cause a power imbalance in the AC grid, which causes a frequency variation in the whole system, but locally each generator will provide a different response, based on the electrical distance of the SG connect to the PCC. The response also depends on the rated power of the machine and the operating point at the moment of the disturbance. In general, as shorter is the electrical distance of the SG, bigger is impact of the local RoCoF, meaning that the response of the converter is going to be stronger when compared with farther electrical distances. The main implication of the local RoCoF is that the SG can trigger its protection actions based of the local measurement of frequency, resulting is unforeseen disconnection of generators in the grid. Therefore, the local RoCoF can be considered a suitable index to measure the impacts of DC faults in the HVDC system context.

#### 5.1.5. Possibilities of energy resource allocation

A possible solution for the allocation of energy resources is to oversize the converters dedicated to support the AC grid, increasing the capacity of the converter to provide support to the network. The strategy of oversizing converters capacity creates extra headroom that can be utilized for providing ancillary services, such as frequency support (inertial response in VSM converters) and voltage support to enhance the system stability. The concept involves maintaining the existing grid configuration while increasing the nominal power capacity of the converters (e. g. 20% capacity increase in this study). Importantly, this approach does not require adjustments to the sizing of surrounding equipment and cables, allowing the overall system to retain its original size. The additional power capacity is intended

for transient use only. Consequently, the system can continue to provide support to the AC grid even when the converter is fully dispatched, providing an additional operational margin for voltage and frequency support. This approach is particularly notable when employing GFM control of the converters, especially in VSM strategy. In conclusion, the oversizing strategy provides the extra power headroom exclusively to AC grid support, which is a good advantage, extending the limits of power support of the converter and reducing the impacts in the AC grid, but as the overload capacity of the converter is much lower when compared to a synchronous machine. Usually, the converter has a transient overload capacity of up to 1.2 times its rated capacity, while synchronous generators provide overload current up to 6 times their rated capacity in a contingency event, e.g. faults transients. This difference remains crucial for fault ride-through operation and plays an important role to support the grid during fault events, which still limits the response of the converter, and its inherent design constrains when compared with synchronous machines.

Another possible solution for the allocation of energy resources is to include Energy Storage System (ESS) in the AC grid as a Frequency Containment Reserve (FCR). The available energy from the ESS can be used to reduce the power mismatch into the AC grid during disturbances in the DC system. Therefore, the impacts in the AC grid, such as frequency and voltage variations should be reduced thanks to the available power in the ESS. The response of the ESS is directly related to its dynamic response, which can be considered quite fast if a lithium battery-based storage system is used, with a time constant of 20 ms, sufficient to compensate for a disturbance in an AC grid. Another important characteristic is the activation time of the ESS. In this case, a delay of 10 ms between the opening of the DCCB and the activation of the ESS was considered. Additionally, a ramp of 100 ms is needed to reach the given reference, so the ESS takes 120 ms to reach the reference value from the beginning of the disturbance. Therefore, considering this response time, the ESS can be a good solution to improve the frequency nadir, gaining an advantage for its steady-state value. It is also possible to improve the voltage value in steady state. However, in these conditions it is not sufficient to improve the initial frequency transient, which would require faster reaction from the ESS to support the enhancement of the RoCoF. A suitable solution could be the application of ESS in GFM control or even to be triggered by established RoCoF limits.

#### 5.1.6. Issues in PE based grids

In the context of Power Electronics (PE) based grids, the absence of rotating machines directly impacts the system's inertia, resulting in a significant reduction. Consequently, implementing Grid Forming (GFM) strategies in PE grids becomes crucial to uphold system stability, particularly concerning frequency and voltage control, which are shared among the converters connected to the grid. Moreover, the operation of DC Fault Ride Through (FRT) is influenced by grid characteristics, altering the effect of DC faults when the converter station is integrated into a PE grid. In such scenarios, converters exhibit limited overload capacity. During a DC fault, the power profile necessary to supply the DC grid is distributed among the converters based on their power availability and electrical distance. In weak grids ( $SCR < 3$ ), the closest healthy converter to the faulty one (healthy pole) bears the brunt of supporting the DC FRT operation due to the substantial power demand from the AC side of the grid. However, this surge in power can trigger overload responses in the healthy pole, activating current saturation algorithms or even causing converter blocking. This implies that faulty converters in PE grids may not experience excessively high current faults like in traditional grids where the fault currents are the initial trigger of the FRT. In this case, the blocking of faulty converters is triggered by DC voltage levels rather than current. Additionally, the response of grid converters located at longer electrical distances is not as significant, as they are unable to provide the same level of power response as healthy converters due to the substantial reduction in power flow capacity within weak grids. In

summary, PE grids have limited capability to support DC FRT operations, with efforts primarily concentrated on the healthy converter in a bipolar configuration. Nonetheless, the combined use of GFM strategies and current limitation through virtual impedance approaches effectively manages such disturbances, ensuring grid stability during FRT events.

## AC Protection Impacts Conclusions

The study investigates the challenges posed by the integration of converters into high-voltage AC grids, focusing specifically on their impact on distance protection relays. The findings indicate that converter-based resources present significant challenges for traditional protection schemes, leading to potential reliability issues, such as under-reaching or over-reaching during grid disturbances.

Converter behaviour during fault conditions is largely determined by their control structures, which differ significantly from traditional SGs. Control modes as GFL or GFM exhibit dynamic impedance characteristics that could impact the accuracy and reliability of distance protection relays. These differences between GFL and GFM converters can result in faults being detected too late (under-reach) or incorrectly (over-reach), necessitating careful tuning of distance protection relays. GFL control tends to exhibit greater variations in fault impedance compared to GFM control, posing additional challenges for protection systems. The study also observed that the transient behaviour of a converter's fault response, particularly within the first milliseconds of a fault, is crucial for the relay's performance. The proximity of the converter to the fault affects the measured fault-loop impedance. Furthermore, the impact of converter bandwidth, current-limitation methods, and virtual impedance control requires further investigation to enhance the performance of protection systems. Additionally, resistive faults and shifts in fault-loop impedance caused by converter behaviour, particularly in meshed grids, introduce additional complexities for protection relays. An overview of these general outcomes is provided in Table 3-3.

The study employed a simplified test network, based on the IEEE 9-bus system, which was modified to integrate both SGs and converters. This setup was used to evaluate the performance of protection devices under varying conditions, including different control strategies and grid configurations. The simulations highlighted potential malfunctions in distance protection relays related to factors such as converter control bandwidth and fault current limitations. The network provided a foundation for exploring these challenges and can be used for more detailed studies in Work Package 7.

Future work should concentrate on more complex grid configurations, including higher levels of converter integration, different control strategies, and varied grid topologies. Specifically, future investigations should focus on Use Case 1 (WP7.1), which deals with a highly meshed AC grid and where different combinations of GFM, GFL and SGs operate within the same AC network. These studies will provide insight into how the protection relays behave and will help formulate future recommendations to meet the requirements of the protection system. The focus should also be placed on understanding the correlation between the AC and DC grids, particularly in the context of the AC/DC matrix developed in Work Package 3.1. The growing complexity of DC links, particularly in MTDC systems, and their higher integration into AC systems, has a significant impact on current distance protection strategies.

In summary, while traditional distance protection remains effective in grids dominated by SGs, the increasing presence of converters demands significant adjustments to protection strategies to maintain grid stability and ensure reliable fault detection. Future investigations should explore how AC and DC integration, especially in systems with a high level of converter-based resources, impacts protection schemes and whether new strategies are needed to address these challenges effectively.

**TABLE 5-1: VULNERABILITIES FOR DIFFERENT TOPOLOGIES IN TERMS OF AC PROTECTION.**

DC Grid	DC1				DC2				DC3				DC4			
AC Grid	AC1	AC2a	AC2b	AC3												
Application of distance AC line protection [35]																

The use of distance protection for AC line protection in future grid scenarios may be critical, depending on the DC configuration and AC embedment level from WP3.1. This involves how the DC configuration is structured—whether point-to-point (DC1), radial (DC2), linear (DC3), or meshed (DC4)—and the degree of AC integration. A high embedment level means, that for instance in AC2a, at least two DC converter stations are in the same synchronous AC grid, with one or more separate asynchronous AC grids hosting other DC converter stations, some of which may include offshore wind. In AC2b, the DC system connects two or more separate AC grids, where each grid hosts multiple DC converter stations. In a fully embedded (AC3) scenario, all converter stations of the DC system are connected to the same AC grid. Especially for the AC3 embedment level, the protection system becomes more vulnerable and must be carefully evaluated. However, even in AC2a and AC2b cases, the reliability of protection relays may still be at risk. Therefore, several recommendations should be considered for further investigation in Work Package 7.

### Recommendation

Investigation into different AC grid embedment levels, including various grid topologies such as parallel lines or intermediate infeed, is essential. In addition to the main protection, focus should also be placed on the backup zone element, as the meshed grid configuration and low SCP could jeopardize the reliability of backup protection.

Various AC grid models, integrating MMC with GFL and GFM control strategies, should be further developed. The current simplified model, which uses controlled sources for GFL and GFM, needs to be enhanced with a full electrical model. Therefore, converters should be modelled electrically rather than as controlled sources to investigate the following:

- The role of multiple converters or strong converter dominance (AC/DC matrix)
- The impact of GFL vs. GFM control strategies (and their proportion in the grid)

In addition to integrating different grid topologies and converter control strategies, **the framework conditions** should also be varied to examine:

- Symmetrical and unsymmetrical faults: For unsymmetrical faults, the inverter's operation can affect the negative sequence. As converters are required to inject symmetrical currents to comply with grid codes, this could influence fault detection.
- Grid variation: Factors such as different line lengths and a higher concentration of converters should be explored to assess their impact on the protection system.
- Fault resistance and pre-fault load: The combination of fault resistance and pre-fault load can alter the measured impedance, affecting the relay's response.

- Current reversal: When the current direction reverses, the ability of the relay to detect and maintain functionality can become more challenging.
- DC offset: Converters behave differently from SGs in terms of DC offset. The reduction in the direct current component can distort waveforms, potentially affecting the relay's operation.
- Frequency deviations: Deviations from the standard frequency can disrupt the algorithm of the relay, which are typically calibrated for a specific frequency range. This is particularly impactful for distance protection relays, which rely on the DFT to extract phasors for voltage and current measurements.

By investigating these areas, the study will provide deeper insights into the protection challenges posed by modern grids with high converter integration.

## 5.2. Cyber Security Events Conclusions

This report presents the following key points of conclusion and recommendations for cyber security protection of HVDC grids.

### 1. The importance of the early-stage detection.

According to the literature survey, the state-of-the-art research of cyber security on HVDC grids is primarily focused on the later stage of the cyber kill chain after the adversaries successfully compromise the system, i.e., FDIA, replay attack, spoofing attack, and DoS. The early phase of the cyber kill chain has not been included in state-of-the-art studies. Therefore, in order to enhance the protection of HVDC grids against cyber-attacks, it is crucial to initiate the detection and mitigation process at the earliest stage of the cyber kill chain. Early-stage cyber-attack detection is crucial for minimizing the potential adverse impacts of cyber-attacks in HVDC grids.

### 2. The mitigation strategies must take into account both physical and cyber anomalies.

The state-of-the-art anomaly detections on HVDC grids under cyber-attack are mainly based on physical power system measurement, i.e., SCADA and PMU. The physical anomalies occurred after the cyber-attack had already impacted the physical HVDC grids, during the later stage of the cyber kill chain. Hence, in order to provide a more comprehensive solution, it is imperative to take into account both cyber and physical anomalies when detecting and mitigating anomalies.

### 3. Implementation of secure protocols.

Based on the experimental findings presented in this report, it is evident that the IEC 61850 standard is inadequate in dealing with advanced cyber-attack scenarios. The adversaries have the ability to send an unauthorized command to the digital substation, resulting in the disruption of the HVDC system's operation. Therefore, the implementation of communication should incorporate an integrity checking mechanism to authenticate the source of the command. It is also important to point out that security mechanisms such as the RSA algorithm, which typically functions well in IT systems, may not be effective due to processing time constraints. Therefore, the forthcoming implementation of secure communication should incorporate security measures that have a maximum response time of 4 milliseconds.

### 4. Communication time latency constraints.

HVDC cyber-physical systems depend on communication for control and protection schemes. The best-known possible communication media is via fiber optics with a delay of 0.5 ms per 100 km [129], [130]. This delay limit must be considered for implementing HVDC control and protection mechanism. Consequently, in order to make the implementation of cyber security protection and secure protocol application more effective, the solution should minimize the delay in communication. The solution must also take into account the distinct characteristics of OT and IT traffic.

#### **5. Implement throughput-based anomaly detection in the HVDC operational technology network.**

In this report, we present a method to identify anomalies in HVDC communication traffic. The method was developed based on the characteristics of OT communication traffic, which originates from automated processes with deterministic and homogeneous behavior. The method identifies the anomalies based on traffic throughput using a Graph Convolutional Long Short-Term Memory. Subsequently, the results of anomaly detection are combined with the Traffic Dispersion Graph to identify the locations of anomalies. The method is utilized to detect anomalies by analyzing the recorded traffic using a Forensic Graph (FGraph) Model. The proposed FGraph model aligns with the objective of avoiding time delays in HVDC communication by utilizing historical OT traffic data. The results of the experiment indicate the proposed method has the potential to serve as an alternative solution for protecting HVDC systems against cyber-attacks, especially for the early stage of the cyber kill chain.

# Bibliography

- [1] J. C. G. Torres, "Transient stability of high voltage AC-DC electric transmission systems," Paris-Saclay University, Lyon, 2019.
- [2] E. Spahic, D. Ergin, F. Schettler, J. Dorn and C. Petino, "A closer look at protection concepts for DC systems," in *Cigre*, 2016.
- [3] P. Torwelle, "Development of a HVDC grid protection strategy based on hybrid OHL and cable lines," *PhD Thesis, Université Grenoble Alpes*, p. 245, 2021.
- [4] W. Leterme, *Communication-less protection algorithms for meshed VSC HVDC cable grids*, Leuven: Doctoral Disertation, KU Leuven, 2016.
- [5] A. Zama, A. Bertinato, P. Torwelle, W. L. Garcia, J. V. Doorn, J. P. Kjærgaard, F. Kryezi and A. M. Lindefelt, "North Sea Wind Power Hub Feasibility Study: Methodology For Protection Design (part II)," in *International Conference on Renewable Energies and Smart Technologies*, Albania, 2022.
- [6] D. Liu, D. Tzelepis, A. Dyśko, and C. Booth, "A novel protection scheme for inverter-dominated microgrid," in *15th International Conference on Developments in Power System Protection (DPSP 2020)*, Liverpool, 2020, doi: 10.1049/cp.2020.0023.
- [7] ENTSO-E, "High Penetration of Power Electronic Interfaced Power Sources," ENTSO-E, Brussels, 2017.
- [8] B. R. Oeding and D. Oswald, "Elektrische Kraftwerke und Netze", Munich, Germany: Springer, 2011.
- [9] B. Kroposki et al., "Achieving a 100% Renewable Grid: Operating Electric Power System with Extremely High Levels of Variable Renewable Energy," *IEEE Power and Energy Magazine*, vol. 2, no. 15, pp. 61-73, 2017.
- [10] "HVDC Grid Systems and connected Converter Stations: guideline and parameter lists for functional specifications," CENELEC, 2018.
- [11] "Viking Link Project Overview," Energinet, Denmark, 2019.
- [12] "HVDC-VSC Newsletter," RTE International, France, 2022.
- [13] P. Dworakowski, J. Paez, W. Grieshaber, A. Bertinato and E. Lamard, "Protection of radial MVDC electric network based on DC circuit breaker and DC fuses," *International Journal of Electrical Power & Energy Systems*, vol. 153, p. 109398, 2023.
- [14] M. Ratajczyk, B. Raison and A. Bertinato, "From pole-to-ground fault current return paths in a meshed HVDC network to a grounding modelling simplification for protection studies," *Electric Power Systems Research*, vol. 223, p. 109655, 2023.

- [15] X. Jiang, S. Wang, Q. Zhao and X. Wang, "Exploiting the operational flexibility of AC-MTDC distribution system considering various flexible resources," *International Journal of Electrical Power & Energy Systems*, vol. 148, 2023.
- [16] N. grid, "Review of Grid Code Connection Conditions for Frequency and Voltage Operating Ranges," UK, 2009.
- [17] K. Shinoda, X. Guillaud, S. Bacha, A. Benchaib and B. Francois, "Modelling of a VSC-based multi-terminal HVDC network for dynamic stability analysis," *The international journal for computation and mathematics in electrical and electronic engineering*, vol. 36, no. 1, pp. 240--257, 2017.
- [18] K. Shinoda, "Contrôle et opération des réseaux HVDC multi-terminaux à base de convertisseurs MMC," *Ecole centrale de Lille*, 2017.
- [19] K. Shinoda, A. Benchaib, J. Dai and X. Guillaud, "Virtual Capacitor Control: Mitigation of DC Voltage Fluctuations in MMC-Based HVdc Systems," *IEEE Transactions on Power Delivery*, vol. 33, no. 1, pp. 455-465, 2018.
- [20] K. Shinoda, J. Freytes, A. Benchaib, J. Dai, H. Saad and X. Guillaud, "Energy difference controllers for MMC without DC current perturbations," *The 2nd International Conference on HVDC (HVDC2016)*, 2016.
- [21] K. Shinoda, R. Ramachandran, A. Benchaib, J. Dai, B. François, S. Bacha and X. Guillaud, "Energy Control of Modular Multilevel Converter in MTDC Grids for Wind Power Integration," *17th International Workshop on Large-Scale Integration of Wind Power into Power Systems as well as on Transmission Networks for Offshore Wind Power PlantsAt: Stockholm*, 2018.
- [22] S. D'Arco, J. A. Suul and O. B. Fosso, "Small-signal modelling and parametric sensitivity of a virtual synchronous machine," *IEEE Power Systems Computation Conference*, pp. 1-9, 2014.
- [23] T. Qoria, Grid-forming control to achieve a 100% power electronics interfaced power transmission systems., HESAM Université, 2020.
- [24] S. D'Arco and J. A. Suul, "Equivalence of virtual synchronous machines and frequency-droops for converter-based microgrids," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, 2013.
- [25] J. C. Gonzalez-Torres, R. Mourouvin, K. Shinoda, A. Zama and A. Benchaib, "A simplified approach to model grid-forming controlled MMCs in power system stability studies," in *IEEE PES Innovative Smart Grid Technologies Europe*, Espoo, Finland, 2021.
- [26] R. Mourouvin, K. Shinoda, J. Dai, A. Benchaib, S. Bacha and D. Georges, "AC/DC Dynamic Interactions of MMC-HVDC in Grid-Forming for Wind-Farm Integration in AC Systems," in *22nd European Conference on Power Electronics and Applications (EPE'20 ECCE Europe)*, Lyon, France, 2020.
- [27] P. Torwelle, A. Bertinato and T. L. M. P. B. Raison, "Fault current calculation in MTDC grids considering MMC blocking," *Electric Power Systems Research*, vol. 207, no. Elsevier, p. 07662, 2022.

- [28] F. Sadeque, D. Sharma and B. Mirafzal, "Seamless Grid-Following to Grid-Forming Transition of Inverters Supplying a Microgrid," in *IEEE Applied Power Electronics Conference and Exposition (APEC)*, Orlando, 2023.
- [29] J. Wang, S. Ganguly and B. Kroposki, "Study of Seamless Microgrid Transition Operation Using Grid-Forming Inverters," in *49th Annual Conference of the IEEE Industrial Electronics Society*, Singapore, 2023.
- [30] T. Qoria, F. Gruson, F. Colas and X. Kestelyn, "Current limiting algorithms and transient stability analysis of grid-forming VSCs," *Electric Power Systems Research*, vol. 189, p. 106726, 2020.
- [31] A. D. Paquette and D. M. Divan, "Virtual impedance current limiting for inverters in microgrids with synchronous generators," *IEEE Transactions on Industry Applications*, vol. 51, no. 2, pp. 1630--1638, 2014.
- [32] G. Denis, "From grid-following to grid-forming: The new strategy to build 100% power-electronics interfaced transmission system with enhanced transient behavior," *EC-Lille, Ph. D*, vol. 23, 2017.
- [33] E. Turbines, "EUTurbines position paper on RoCoF related questions," European Association of Gas and Steam Turbine Manufacturers, Brussels, 2022.
- [34] J. Vieira, W. Freitas, W. Xu and M. A., "Efficient coordination of ROCOF and frequency relays for distributed generation protection by using the application region," *IEEE transactions on power delivery*, vol. 21, no. 4, pp. 1878-1884, 2006.
- [35] N. Baeckeland, Doctoral Thesis: Design and Modeling of Inverter Control for Fault Behavior and Power System Protection Analysis, 2022.
- [36] J. L. Blackburn, Protective Relaying: Principles and Applications, Fourth Edition, Baton Rouge: Taylor & Francis Group, 2014.
- [37] J. Machowski et al, Power system dynamics. Stability and control, Hoboken, NJ, USA: John Wiley, 2020.
- [38] S.H. Horowitz, A. G. Phadke, C.F. Henville, Power system relaying, West Sussex, UK: John Wiley & Sons, 2023.
- [39] G. Ziegler, Numerical distance protection. Principles and applications, Erlange: Publicis Publ, 2011.
- [40] J.D. Glover, M. S. Sarma, T. J. Overbye, Power system analysis and design, 2012: Cengage Learning, Australia.
- [41] J. Zheng, P. Li, K. Xu, X. Kong, C. Wang, J. Lin and C. Zhang, "A distance protection scheme for HVDC transmission lines based on the Steady-state parameter model," *International Journal of Electrical Power & Energy Systems*, vol. 136, 2022.
- [42] Prof. Dr. Uwe Leprich Dr.-Ing. Michael Ritzau Prof. Dr.-Ing. Michael Igel, "Ausbau elektrischer Netze mit Kabel oder Freileitung unter besonderer Berücksichtigung der Einspeisung

Erneuerbarer Energien. Eine Studie im Auftrag des Bundesministeriums für Umwelt, Naturschutz und Reaktorsicherheit," 2011.

- [43] IEC 60255-121:2014, "Measuring relays and protection equipment - Part 121: Functional requirements for distance protection," NORME EUROPÉENNE, 2014.
- [44] C. Brantl, "Impact factors on the 2nd zone of distance protection under integration of modular multilevel converters," in *54th International Universities Power Engineering Conference (UPEC)*, Bucharest, 2019, doi: 10.1109/UPEC.2019.8893639.
- [45] M.M. Alam, H.Leite, N. Silva, and A. da Silva Carvalho, "Performance evaluation of distance protection of transmission lines connected with vsc-hvdc system using closed loop test in rtds," *Electric Power System Research*, no. 152, pp. 168-183, 2017.
- [46] C. Brantl, P. Ruffing and R. Puffer, "The application of line protection relays in high voltage AC transmission grids considering the capabilities and limitations of connected MMCs," in *15th International Conference on Developments in Power System Protection (DPSP 2020)*, Liverpool, 2020, doi: 10.1049/cp.2020.0062.
- [47] O. D. Naidu, N. George, S. Zubic and M. Krakowski, "Time-Domain-Based Distance Protection for Transmission Networks: Secure and Reliable Solution for Complex Networks," *IEEE Access*, vol. 11, pp. 104656-104675, 2023.
- [48] Chakrapani, Venkatesh; Voloh, Ilia; Horton, Patricia; Swain, Simon, "Assessing the performance of an enhanced distance relay in converter-dominated network," in *17th International Conference on Developments in Power System Protection (DPSP 2024)*, Manchester, UK, 2024.
- [49] S. Cao, Q. Hong, D. Liu, L. Ji and C. Booth, "Impact of converter equivalent impedance on distance protection with the MHO characteristic," in *17th International Conference on Developments in Power System Protection (DPSP 2024)*, Manchester, UK, 2024.
- [50] I. Boldea, *Electric Generators Handbook - Two Volume Set*, Boca Raton: Chapman and Hall/CRC, 2015.
- [51] A. Haddadi, I. Kocar, J. Mahseredjian, U. Karaagac, and E. Farantatos, "Performance of Phase Comparison Line Protection Under Inverter-Based Resources and Impact of the German Grid Code," in *IEEE Power & Energy Society General Meeting (PESGM)*, Montreal, QC, Canada, 2020.
- [52] Hani A. Alkhazim et al., "Impact of Inverter Based Resources on Power System Protective Relaying, Fault Calculation and Protection Setting: A Systematic Literature Review," in *Saudi Arabia Smart Grid (SASG)*, Riyadh, 2022.
- [53] P. M. Anderson and A. A. Fouad, *Power System Control and Stability*, Wiley-IEEE Press, 2003.
- [54] PSCAD, "IEEE 09 Bus System," Manitoba Hydro International Ltd., 22 February 2022. [Online]. Available: <https://www.pscad.com/knowledge-base/article/25>.

- [55] J. Girona-Badia, et al, “Design, Control and Testing of a Modular Multilevel Converter with a Single Cell per Arm in Grid-Forming and Grid-Following Operations for Scaled-Down Experimental Platforms,” *Energies*, vol. 5/15, p. 1819, 2022.
- [56] E. Rokrok, “Grid-forming control strategies of power electronic converters in transmission grids: application to HVDC link; Doctoral Thesis,” Centrale Lille Institut, Lille, 2022.
- [57] F. Blaabjerg et al., “Overview of Control and Grid Synchronization for Distributed Power Generation Systems,” *IEEE Transactions on Industrial Electronics*, vol. 5, no. 53, p. 1398–1409, 2006.
- [58] X. Gao et al., “Comparative Study of Grid-Following and Grid-Forming Control Schemes in Power Electronic-Based Power Systems,” *Power Electronics and Drives*, vol. 1, no. 8, pp. 1-20, 2023..
- [59] Y. Li ; Y. Gu; T. C. Green, “Revisiting Grid-Forming and Grid-Following Inverters: A Duality Theory,” *IEEE TRANSACTIONS ON POWER SYSTEMS*, vol. 37, no. 6, 2022.
- [60] A. Yazdani, Voltage-sourced converters in power systems. Modeling, control, and applications, Hoboken, N.J., US: IEEE Press/Wiley, 2010.
- [61] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. MihetPopa, “Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications,” *IEEE Access*, vol. 8, p. 151019–151064, 2020.
- [62] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, “A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future,” *Electric Power Systems Research*, vol. 215, p. 108975, 2023.
- [63] T. Huang, B. Satchidanandan, P. R. Kumar, and L. Xie, “An Online Detection Framework for Cyber Attacks on Automatic Generation Control,” *IEEE Transactions on Power Systems*, vol. 33, no. 6, p. 6816–6827, 2018.
- [64] A. S. L. V. Tummala and R. K. Inapakurthi, “A two-stage kalman filter for cyber-attack detection in automatic generation control system,” *Journal of Modern Power Systems and Clean Energy*, vol. 10, no. 1, pp. 50-59, 2022.
- [65] M. Zhou, C. Liu, A. A. Jahromi, D. Kundur, J. Wu, and C. Long, “Revealing Vulnerability of N-1 Secure Power Systems to Coordinated Cyber-Physical Attacks,” *IEEE Transactions on Power Systems*, vol. 38, no. 2, p. 1044–1057, 2023.
- [66] Y. Yang, G. Raman, J. C.-H. Peng, and Z.-S. Ye, “Resilient Consensus- Based AC Optimal Power Flow Against Data Integrity Attacks Using PLC,” *IEEE Transactions on Smart Grid*, vol. 13, no. 5, p. 3786–3797, 2022.
- [67] C. Tu, X. He, X. Liu, and P. Li, “Cyber-Attacks in PMU-Based Power Network and Countermeasures,” *IEEE Access*, vol. 6, p. 65594–65603, 2018.

- [68] S. De Silva, J. Kim, E. Cotilla-Sanchez, and T. Hagan, "On PMU Data Integrity Under GPS Spoofing Attacks: A Sparse Error Correction Framework," *IEEE Transactions on Power Systems*, vol. 36, no. 6, p. 5317–5332, 2021.
- [69] V. S. Rajkumar, M. Tealane, A. Stefanov, and P. Palensky, "Cyber Attacks on Protective Relays in Digital Substations and Impact Analysis," in *8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*, Delft, 2020.
- [70] I. Siniosoglou, P. Radoglou-Grammatikis, G. Efstathopoulos, P. Fouliras, and P. Sarigiannidis, "A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, p. 1137–1151, 2021.
- [71] X. Liang and M. Abbasipour, "HVDC Transmission and its Potential Application in Remote Communities: Current Practice and Future Trend," *IEEE Transactions on Industry Applications*, vol. 58, no. 2, p. 1706–1719, 2022.
- [72] Y. Xu, Y. Yang, T. Li, J. Ju, and Q. Wang, "Review on cyber vulnerabilities of communication protocols in industrial control systems," in *IEEE Conference on Energy Internet and Energy System Integration (EI2)*, 2017.
- [73] S. Sahoo, T. Dragicevic, and F. Blaabjerg, "Cyber security in control of grid-tied power electronic converters - challenges and vulnerabilities," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 5, pp. 5326-5340, 2021.
- [74] A. Gholami, M. Mousavi, A. K. Srivastava, and A. Mehrizi-Sani, "Cyber- Physical Vulnerability and Security Analysis of Power Grid with HVDC Line," in *North American Power Symposium (NAPS)*, 2019.
- [75] J. Hatton, B. K. Johnson, D. Roberson, and R. Nuqui, "Increased Grid Resilience Via Cyber-Secure VSC Multiterminal HVDC Systems," in *IEEE Power Energy Society General Meeting (PESGM)*, 2019.
- [76] . Zhang, J. Li, Y. Xing, O. Bamisile, and Q. Huang, "Data-driven load frequency cooperative control for multi-area power system integrated with vsacs and ev aggregators under cyber-attacks," *ISA transactions*, vol. 143, p. 440–457, 2023.
- [77] A. Devnath, M. Rahman, and M. Rana, "Impact analysis of cyber-attack on mmc-hvdc control system with countermeasures," *International Journal of Dynamics and Control*, pp. 1-11, 2023.
- [78] J. Hou, S. Lei, Y. Song, L. Zhu, W. Sun, and Y. Hou, "The cost and benefit of enhancing cybersecurity for hybrid ac/dc grids," *IEEE Transactions on Smart Grid*, vol. 14, no. 3, pp. 4758-4771, 2023.
- [79] R. Fan, J. Lian, K. Kalsi, and M. A. Elizondo, "Impact of cyber attacks on high voltage dc transmission damping control," *Energies*, vol. 11, no. 5, p. 1046, 2018.

- [80] A. A. Aljabrine, A. A. Smadi, Y. Chakhchoukh, B. K. Johnson, and H. Lei, "Resiliency improvement of an ac/dc power grid with embedded lcc-hvdc using robust power system state estimation," *Energies*, vol. 14, no. 23, p. 7847, 2021.
- [81] J. Hou, S. Lei, W. Yin, W. Sun, and Y. Hou, "Cybersecurity enhancement for multi-infeed high-voltage dc systems," *IEEE Transactions on Smart Grid*, vol. 13, no. 4, p. 3227–3240, 2022.
- [82] Q. Jiang, B. Li, T. Liu, F. Blaabjerg, and P. Wang, "Study of cyber attack's impact on lcc-hvdc system with false data injection," *IEEE Transactions on Smart Grid*, vol. 14, no. 4, pp. 3220–3231, 2023.
- [83] T. Ding, "Quantifying Cyber Attacks on Industrial MMC-HVDC Control System Using Structured Pseudospectrum," *IEEE Transactions on Power Electronics*, vol. 36, no. 5, p. 4915–4920, 2021.
- [84] C. Burgos-Mellado, "Cyber-attacks in modular multilevel converters," *IEEE Transactions on Power Electronics*, vol. 37, no. 7, p. 8488–8501, 2022.
- [85] J. Cao, C. Dong, X. Yu, R. Wang, Q. Xiao, and H. Jia, "Modelling and stability assessment of the mmc-hvdc energy interconnected system with the cyber delay of communication network," *IET Energy Systems Integration*, vol. 3, no. 1, 2021.
- [86] J. Cao, C. Dong, X. Yu, Y. Mu, Q. Xiao, and H. Jia, "Modeling and Rekasius substitution stability analysis of the multi-terminal MMC-HVDC cyber-physical system," in *IEEE Energy Conversion Congress and Exposition (ECCE)*, 2021.
- [87] K. Pan, J. Dong, E. Rakhshani, and P. Palensky, "Effects of Cyber Attacks on AC and High-Voltage DC Interconnected Power Systems with Emulated Inertia," *Energies*, vol. 13, no. 21, 2020.
- [88] K. Pan, E. Rakhshani, and P. Palensky, "False Data Injection Attacks on Hybrid AC/HVDC Interconnected Systems With Virtual Inertia—Vulnerability, Impact and Detection," *IEEE Access*, vol. 8, p. 141932–141945, 2020.
- [89] B. Chen, S.-i. Yim, H. C. Kim, and R. Nuqui, "Cyber Attack Detection for WAMPAC-based HVDC Applications," in *IEEE/PES Transmission and Distribution Conference and Exposition*, 2020.
- [90] . Chen, S.-i. Yim, H. Kim, A. Kondabathini, and R. Nuqui, "Cybersecurity of Wide Area Monitoring, Protection, and Control Systems for HVDC Applications," *IEEE Transactions on Power Systems*, vol. 36, no. 1, p. 592–602, 2021.
- [91] K. Sun, W. Qiu, W. Yao, S. You, H. Yin, and Y. Liu, "Frequency Injection Based HVDC Attack-Defense Control Via Squeeze-Excitation Double CNN," *IEEE Transactions on Power Systems*, vol. 36, no. 6, pp. 5305–5316, 2021.
- [92] W. Qiu, K. Sun, W. Yao, W. Wang, Q. Tang, and Y. Liu, "Hybrid Data-Driven Based HVDC Ancillary Control for Multiple Frequency Data Attacks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 12, p. 8035–8045, 2021.

- [93] S. D. Roy, S. Debbarma, and J. M. Guerrero, "Machine learning based multi-agent system for detecting and neutralizing unseen cyber-attacks in ac and hvdc systems," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 12, no. 1, pp. 182-193, 2022.
- [94] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 446-464, 2016.
- [95] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (cpps): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, p. 151019–151064, 2020.
- [96] Y. Zhao, W. Yao, C.-K. Zhang, X.-C. Shangguan, L. Jiang, and J. Wen, "Quantifying resilience of wide-area damping control against cyber attack based on switching system theory," *IEEE Transactions on Smart Grid*, vol. 13, no. 3, p. 2331–2343, 2022.
- [97] Y. Zhao, W. Yao, C.-K. Zhang, X. Ai, and J. Wen, "Resilient wide-area damping control to mitigate strong cyber attack: A multiple-controller switching approach," *IEEE Transactions on Smart Grid*, vol. 14, no. 3, p. 2326–2337, 2022.
- [98] Y. Jiang, S. Wu, H. Yang, H. Luo, Z. Chen, S. Yin, and O. Kaynak, "Secure data transmission and trustworthiness judgement approaches against cyber-physical attacks in an integrated data-driven framework," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 12, p. 7799–7809, 2022.
- [99] W. Yao, J. Nan, Y. Zhao, J. Fang, X. Ai, W. Zuo, J. Wen, and S. Cheng, "Resilient wide-area damping control for inter-area oscillations to tolerate deception attacks," *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4238-4249, 2021.
- [100] R. Hemmati and H. Faraji, "Multifunctional scheme for frequency/voltage/stability control in hvdc line under concurrent cyber-attacks and faults," *IET Generation, Transmission & Distribution*, vol. 16, no. 7, 2022.
- [101] Y. Zhao, W. Yao, J. Nan, J. Fang, X. Ai, J. Wen, and S. Cheng, "Resilient adaptive wide-area damping control to mitigate false data injection attacks," *IEEE Systems Journal*, vol. 15, no. 4, p. 4831–4842, 2020.
- [102] Y. Shen, W. Yao, J. Wen, H. He, and L. Jiang, "Resilient wide-area damping control using grhdp to tolerate communication failures," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2547-2557, 2019.
- [103] J. M. Hendrickx, K. H. Johansson, R. M. Jungers, H. Sandberg, and K. C. Sou, "Efficient computations of a security index for false data attacks in power networks," *IEEE Transactions on Automatic Control*, vol. 59, no. 12, pp. 3194-3208, 2014.
- [104] A. Ameli, A. Hooshyar, E. F. El-Saadany, and A. M. Youssef, "Attack detection and identification for automatic generation control systems," *IEEE Transactions on Power Systems*, vol. 33, no. 5, p. 4760–4774, 2018.

- [105] R. Nuqui, H. Lee, A. Kondabathini, M. Overeem, and J. Barton, "Cyber Secured Power Orders for Resilient HVDC Systems," in *IEEE/PES Transmission and Distribution Conference and Exposition*, 2020.
- [106] B. Chen, S.-i. Yim, H. Kim, A. Kondabathini, and R. Nuqui, "Cybersecurity of Wide Area Monitoring, Protection, and Control Systems for HVDC Applications," *IEEE Transactions on Power Systems*, vol. 36, no. 1, p. 592–602, 2021.
- [107] K. Sun, "Wams-based hvdc damping control for cyber attack defense," *IEEE Transactions on Power Systems*, vol. 38, no. 1, pp. 702-713, 2022.
- [108] C. L. Page, B. K. Johnson, D. Roberson, and R. Nuqui, "Increasing grid resilience via cyber-secure series multi-terminal lcc hvdc transmission systems," in *52nd North American Power Symposium*, 2021.
- [109] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber- induced power outage: Analysis and practical mitigation strategies," in *70th Annual Conference for Protective Relay Engineers*, 2017.
- [110] M. J. Assante, R. M. Lee, and T. Conway, "Ics defense use case no. 6: Modular ics malware," SANS, 2017.
- [111] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence- driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," Lockheedmartin, 2011.
- [112] J. Hou, S. Lei, W. Yin, C. Peng, and Y. Hou, "Optimal Cyber Defense Strategy of High-Voltage DC Systems for Frequency Deviation Mitigation," in *SmartGridComm*, 2020.
- [113] H. Ronellenfitsch, M. Timme, and D. Witthaut, "A Dual Method for Computing Power Transfer Distribution Factors," *IEEE Transactions on Power Systems*, vol. 32, no. 2, pp. 1007-1015, 2017.
- [114] R. R. Barbosa, R. Sadre, and A. Pras, "Difficulties in modeling scada traffic: a comparative analysis," in *Passive and Active Measurement: 13th International Conference*, Vienna, 2012.
- [115] E. S. Pilli, R. C. Joshi, and R. Niyogi, "Network forensic frameworks: Survey and research challenges," *digital investigation*, vol. 7, no. 1, pp. 14-27, 2010.
- [116] V. T. Guimaraes, C. M. D. S. Freitas, R. Sadre, L. M. R. Tarouco, and L. Z. Granville, "A survey on information visualization for network and service management," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, p. 285–323, 2015.
- [117] R. Shi, M. Yang, Y. Zhao, F. Zhou, W. Huang, and S. Zhang, "A matrix- based visualization system for network traffic forensics," *IEEE Systems Journal*, vol. 10, no. 4, p. 1350–1360, 2015.
- [118] M. Iliofotou, P. Pappu, M. Faloutsos, M. Mitzenmacher, S. Singh, and G. Varghese, "Network monitoring using traffic dispersion graphs (tdgs)," in *Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, 2007.

- [119] D. Q. Le, T. Jeong, H. E. Roman, and J. W.-K. Hong, "Traffic dispersion graph based anomaly detection," in *Proceedings of the 2nd Symposium on Information and Communication Technology*, 2011.
- [120] Z. Cui, K. Henrickson, R. Ke, and Y. Wang, "Traffic graph convolutional recurrent neural network: A deep learning framework for network-scale traffic learning and forecasting," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 11, p. 4883–4894, 2019.
- [121] J. Chen, X. Wang, and X. Xu, "Gc-lstm: Graph convolution embedded lstm for dynamic network link prediction," *Applied Intelligence*, pp. 1-16, 2022.
- [122] H.S. Wu, "A survey of research on anomaly detection for time series," in *International Computer Conference on Wavelet Active Media Technology and Information Processing*, 2016.
- [123] P. P. Biswas, H. C. Tan, Q. Zhu, Y. Li, D. Mashima and B. Chen, "A Synthesized Dataset for Cybersecurity Study of IEC 61850 based Substation," in *IEEE SmartGridComm*, Beijing, 2019.
- [124] S. Myneni, A. Chowdhary, A. Sabur, S. Sengupta, G. Agrawal, D. Huang, "DAPT 2020—Constructing a benchmark dataset for advanced persistent threats," in *Deployable Machine Learning for Security Defense*, Springer Int, 2020, pp. 138-163.
- [125] A. Presekal, A. Stefanov, V. S. Rajkumar, and P. Palensky, "Attack graph model for cyber-physical power systems using hybrid deep learning," *IEEE Transactions on Smart Grid*, vol. 14, no. 5, p. 4007–4020, 2023.
- [126] IEC 61850-8-1-2011, "IEC Standard for Communications Networks and Systems for Power Utility Automation—Part 8-1: Specific Communication Service Mapping (SCSM)—Mappings to MMS (ISO 9506–1 and ISO 9506-2) and to ISO/IEC 8802-3," IEC, 2011.
- [127] S. M. S. Hussain, S. M. Farooq and T. S. Ustun, "Analysis and Implementation of Message Authentication Code (MAC) Algorithms for GOOSE Message Security," *IEEE Access*, vol. 7, pp. 80980-80984, 2019.
- [128] S. M. S. Hussain, T. S. Ustun and A. Kalam, "A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 5643-5654, 2020.
- [129] M. Muniappan, "A comprehensive review of dc fault protection methods in hvdc transmission systems," *Protection and Control of Modern Power Systems*, vol. 6, no. 1, p. 1, 2021.
- [130] M. Perez-Molina, D. Larruskain, P. E. Lopez, G. Buigues, and V. Valverde, "Review of protection systems for multi-terminal high voltage direct current grids," *Renewable and Sustainable Energy Reviews*, vol. 144, p. 111037, 2021.
- [131] M. Abedrabbo, M. Wang, P. Tielens, F. Zerihun, W. Leterme, J. Berteen and D. V. Hertem, "Impact of DC grid contingencies on AC system stability," 2017.
- [132] D. Zhou, M. H. Rahman, L. Xu and Y. Wang, "Impact of DC protection strategy of large HVDC network on frequency response of the connected AC system," *The journal of engineering*, pp. 4031-4035, 2019.

- [133] J. Dave, H. Ergun and D. V. Hertem, "Incorporating DC grid protection, frequency stability and reliability into offshore DC grid planning.," *IEE Transactions on Power Delivery*, vol. 35, no. 6, pp. 2772-2781, 2020.
- [134] C. Brantl, M. Knechtges, P. Düllman, C. Maier and A. Moser, "Requirements on offshore HVDC grid protection: Interaction with ac system inertia and fast frequency support," 2021.
- [135] P. Kundur, *Power system stability and control*, Palo Alto: McGraw-Hill, 1993.
- [136] R. Feldman, E. Farr, A. J. Watson, J. C. Clare, P. Wheeler, D. Trainer and R. W. Crookes, "DC fault ride-through capability and STATCOM operation of a HVDC hybrid voltage source converter," *IET Generation, Transmission & Distribution*, vol. 8, no. 1, pp. 114-120, 2014.
- [137] J. A. Ansari, C. Liu and S. A. Khan, "MMC based MTDC grids: A detailed review on issues and challenges for operation, control and protection schemes," *IEEE Access*, vol. 8, 2020.
- [138] L. Shi, G. P. Adam, R. Li and L. Xu, "Enhanced control of offshore wind farms connected to MTDC network using partially selective DC fault protection," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 3, pp. 2926-2935, 2020.
- [139] S. Zhang, F. G. G. Zou, X. Wei and C. Zhou, "A Comprehensive Review of Multiport DC Circuit Breakers for MTdc Grid Protection," *IEEE Transactions on Power Electronics*, 2023.
- [140] P. Verrax, P. Torwelle, A. Bertinato, J. V. DOORN and F. KRYEZI, "North Sea Wind Power Hub pre-FEED study: HVDC grid active power loss and restoration requirements based on AC frequency stability assessment," in *B4 International SC Meeting and Colloquium*, Vienna, 2023.
- [141] B. Luscan, S. Bacha, A. Benchaib, A. Bertinato, J. C. G.-T. L. Chédot, S. Poullain, M. Romero-Rodriguez and K. Shinoda, "A vision of HVDC key role toward fault-tolerant and stable AC/DC grids," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 6, pp. 7471-7485, 2020.
- [142] A. Haddadi, M. Zhao, I. Kocar, U. Karaagac, K. W. Chan, and E. Farantatos,, "Impact of Inverter-Based Resources on Negative Sequence Quantities-Based Protection Elements," *IEEE Transactions on Power Delivery*, vol. 36, no. 1, p. 289–298, 2021.