Chapter 3

A Cyber Resilient Protection Scheme for Bipolar DC Microgrids

A DC microgrid may be unipolar or bipolar. A unipolar system is simple to implement and has no voltage asymmetry, whereas a voltage balancer circuit is required in a bipolar DC microgrid to overcome any potential asymmetry between the two pole voltages [9]. Furthermore, in case of asymmetry between the positive and negative poles, current flows through the neutral. As a result, a neutral conductor is needed since ground currents are typically prohibited because they lead to corrosion [10]. Such a configuration is helpful for supplying the load at three different voltage levels $V_{dc}, -V_{dc}$, and $2V_{dc}$. Here, V_{dc} is the magnitude of pole-to-ground voltage. Although the protection of the DC system is challenging to that of a traditional AC system, the presence of enhanced communication infrastructure with eminent processing capacity makes the task easier. However, communication-assisted protection methods are prone to cyber attacks. Thus, there is a scope of development of an improved protection solution for bipolar DC microgrid.

3.1 Introduction

In this chapter, a unit protection scheme for bipolar DC microgrids is proposed which is resilient to cyber attacks. The proposed method uses the current measurement of both ends of the protected line segment to distinguish between internal faults and cyber attacks. For any change in current, the disturbance index exceeds the threshold value, subsequently, the proposed protection algorithm is triggered. Being a bipolar DC sys-

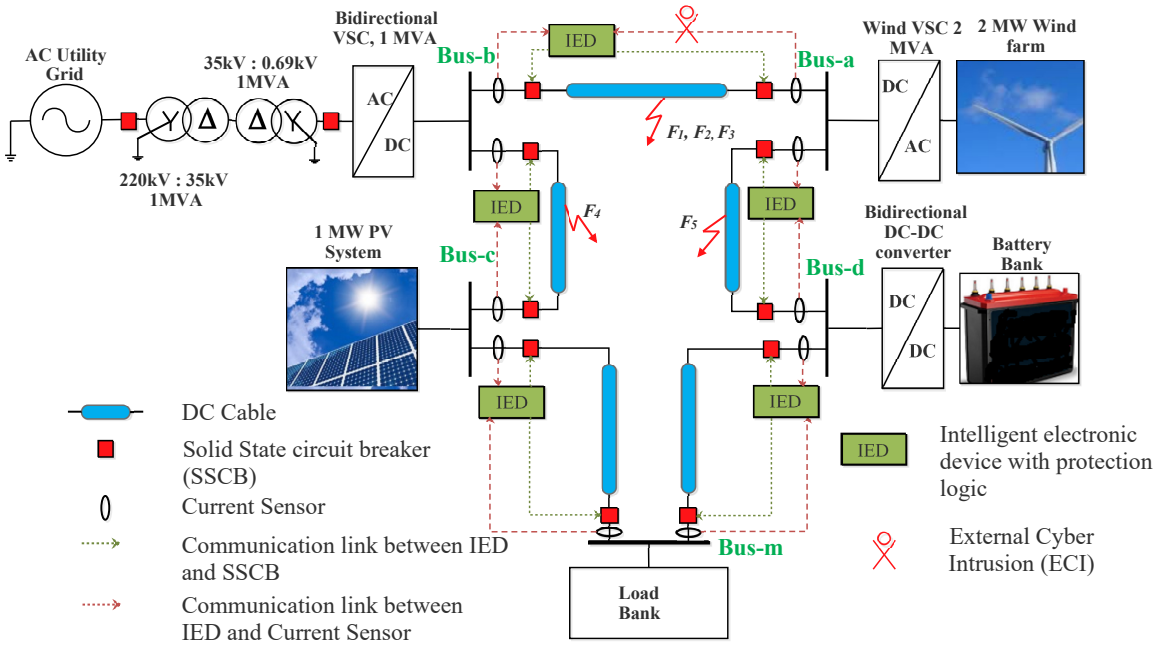


Figure 3.1: A DC ring bus microgrid.

tem, the concept of symmetrical component decomposition is used to obtain the bias, unbalance, and balance components during an unbalance condition. The superimposed balance component of both ends of the line on a four-quadrant plane acts as a decisive discriminator between internal and external faults. The correct faulted pole is identified by analysing the superimposed unbalanced component. By comparing the superimposed bias component with the local pole domain currents, the cyber attack is correctly identified. The proposed protection scheme is validated on a ring-type bipolar DC microgrid, simulated in RTDS, for different internal and external faults and cyber attacks. The performance of the proposed method is tested for various conditions including the detection of internal and external high resistance faults, fault type classification, change in load, distinguishing between different faults and cyber attacks. A comparative assessment of the proposed method with the available techniques confirms its strength. In this work, a cyber resilient protection scheme is proposed that addresses internal fault detection and classification of all possible fault types and sensitivity against cyber attacks in bipolar DC microgrids. The proposed method requires current from both ends of the pole segment for (i) discriminating internal and external faults (ii) fault-type classification (iii) distinguishing cyber attacks from faults. The currents from both ends of the protected line are communicated to the IED, which computes the symmetrical (unbalanced, balanced, and bias) components for protection decisions. Firstly, the disturbance index is obtained by

Table 3.1: Rating of the DC microgrid components [49, 115].

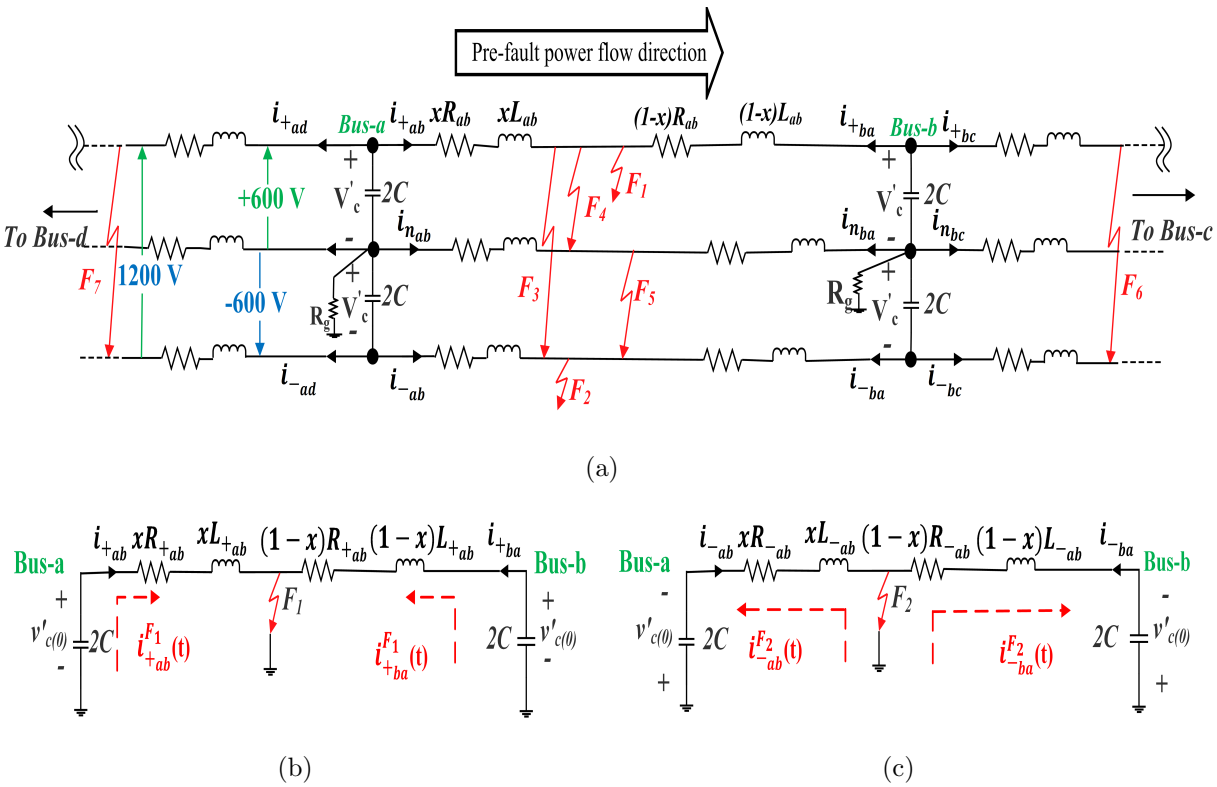
Components	**Ratings**
DC Grid Voltage ($2V_c'$)	1.2 kV ($\pm$ 600 V)
Grid VSC	1 MW
Solar Panel	Vmp = 54.7 V, Imp = 5.58 A at STC
PV Converter	1 MW
Wind Turbine	2 MW PMSG
Wind VSC	2 MW
Battery	300 V, 1.3 kAh, 0.5 MW
Battery VSC	500 kW
DC Link Capacitance ($2C$)	25 mF
Cable Resistance	10 $m\Omega$/km/conductor
Cable Inductance	100 μH/km/conductor
Grounding Resistance (R_g)	0.05 Ω
DC Load	Constant Impedance (2 MW) and, Constant Power (1 MW)

comparing the change in current with a preset threshold. An internal fault is detected when the coordinates of the superimposed balance components are on the first quadrant of Δi-plane. Fault-type classification is accomplished by obtaining the coordinates of superimposed unbalance components. A cyber attack is detected by comparing the superimposed bias components with the superimposed components of the pole domain at the corresponding end. The performance of the proposed method is tested for various cases, including different operating conditions, fault types, and cyber attacks.

3.2 Fault Analysis in a Bipolar DC Microgrids

This section describes the fault current and the respective superimposed current [48] for different faults in a bipolar DC line. It is also explained that the superimposed component of the current-based unit protection method proposed in [48] is not applicable to bipolar DC microgrids.

A bipolar ring bus DC microgrid, as shown in Fig. 3.1 is simulated using RTDS. The parameters of various components of the microgrid are given in Table 3.1. A section of



(a)

(b)

(c)

Figure 3.2: (a) Internal fault in bipolar DC microgrid (b) equivalent circuit PGF (c) equivalent circuit NGF.

the test microgrid is shown in Fig. 3.2(a). The corresponding equivalent circuits during PGF and NGF are given in Fig. 3.2(b) and 3.2(c), respectively. During normal operation (pre-fault), the currents at bus-a ($i_{+_{ab}}$) and at bus-b ($i_{+_{ba}}$) are positive and negative, respectively in the positive pole (as per the sign convention considered in this work). Similarly, in negative pole ($i_{-_{ab}}$) and ($i_{-_{ba}}$) are negative and positive, respectively.

3.2.1 Positive Pole-to-ground fault (PGF)

Consider an internal PGF F_1 at a distance x from bus-a as shown in Fig. 3.2(a). The fault current is the resultant of currents fed by the source and equivalent capacitance in the fault loop. Pre-fault positive pole current seen by the sensor at bus-a, ($i^{pre}_{+_{ab}}$) is positive, and the fault current seen by the positive pole sensor at bus-a is given as [49],

$$i^{F_1}_{+_{ab}}(t) = \frac{v'_C(0)}{L_1\,(s_2 - s_1)}[e^{-s_1 t} - e^{-s_2 t}] + \frac{i_L(0)}{(s_2 - s_1)}[-s_1 e^{-s_1 t} + s_2 e^{-s_2 t}] \tag{3.1}$$

where, $s_1, s_2 = \dfrac{R_1}{L_1} \pm \sqrt{\left(\dfrac{R_1}{L_1}\right)^2 - \dfrac{1}{L_1 C_{eq}}}$. R_1 and L_1 are the equivalent resistance

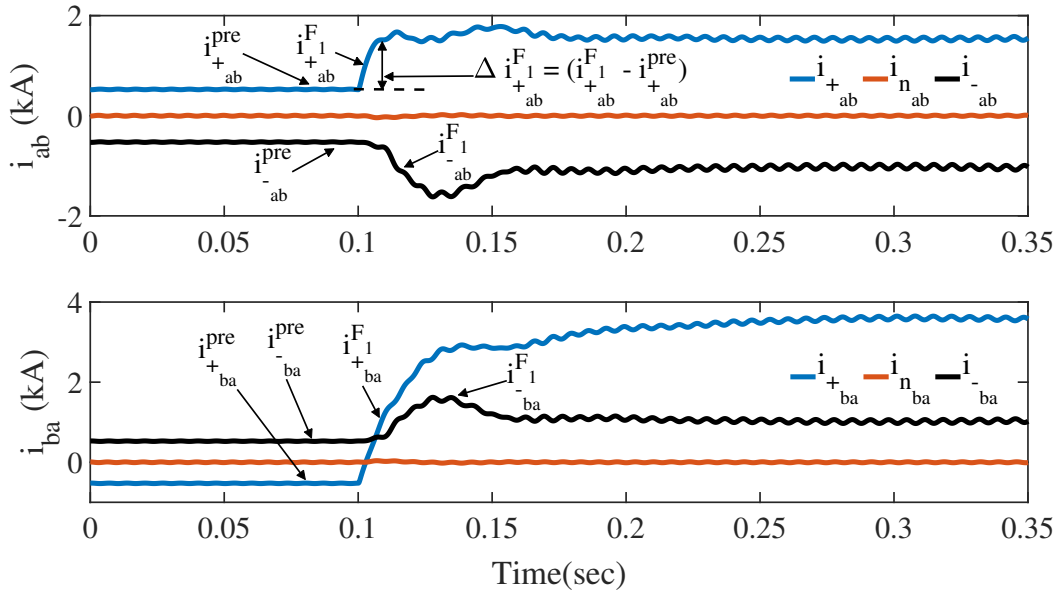


Figure 3.3: Pole domain currents at bus-a and bus-b during PGF (F_1).

and inductance, respectively, in the fault loop. $v_c'(0)$ is the pre-fault voltage across the equivalent capacitance (C_{eq}) in the fault loop.

In this case, the positive pole superimposed current at bus-a ($\Delta i_{+_{ab}}$) for fault F_1 is obtained as

$$\Delta i_{+_{ab}}^{F_1}(t) = i_{+_{ab}}^{F_1}(t) - i_{+_{ab}}^{pre} \tag{3.2}$$

where, $i_{+_{ab}}^{pre} = \dfrac{v_C'(0)}{R_{eq}}$ and $R_{eq} = R_{line} + R_{load}$. At bus-b, the fault current during F_1 ($i_{+_{ba}}^{F_1}$) can be obtained using (3.1). It is evident from (3.2) and Fig. 3.3 that, $\Delta i_{+_{ab}}^{F_1}$ is positive during internal fault F_1. Further, as the convention on the direction of currents as shown in Fig. 3.2(a), during the pre-fault condition, $i_{+_{ba}}^{pre} = -i_{+_{ab}}^{pre}$. From Fig. 3.2(b), it is clear that for internal fault F_1, reading of positive pole sensor at bus-b ($i_{+_{ba}}^{F_1}$) is positive. Therefore the positive pole superimposed current at bus-b ($\Delta i_{+_{ba}}$) during fault F_1 is,

$$\Delta i_{+_{ba}}^{F_1}(t) = i_{+_{ba}}^{F_1}(t) - (-i_{+_{ab}}^{pre}) \tag{3.3}$$

Thus, $\Delta i_{+_{ba}}^{F_1}$ is also positive during internal fault F_1. Similarly, the negative pole current at bus-a ($i_{-_{ab}}$) and bus-b ($i_{-_{ba}}$) are in opposition during F_1 as well as in pre-fault conditions, as shown in Fig. 3.3.

$$\begin{cases} i_{-_{ba}}^{F_1} = -i_{-_{ab}}^{F_1} \\ i_{-_{ba}}^{pre} = -i_{-_{ab}}^{pre} \end{cases} \tag{3.4}$$

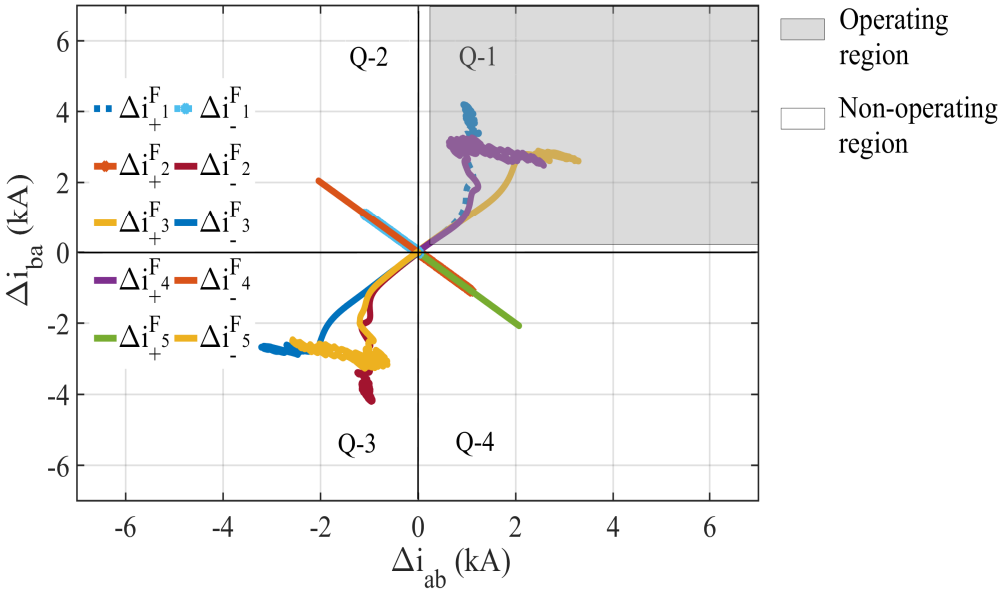


Figure 3.4: Pole domain superimposed currents in Δi-plane for internal faults.

Thus, the negative pole superimposed currents at bus-a ($\Delta i_{-_{ab}}$) and bus-b ($\Delta i_{-_{ba}}$) during F_1 are,

$$\begin{cases} \Delta i^{F_1}_{-_{ab}}(t) = i^{F_1}_{-_{ab}}(t) - i^{pre}_{-_{ab}} \\ \Delta i^{F_1}_{-_{ba}}(t) = -(i^{F_1}_{-_{ab}}(t) - i^{pre}_{-_{ab}}) \end{cases} \tag{3.5}$$

In case of F_1, $\Delta i_{-_{ab}}$ is negative, and $\Delta i_{-_{ba}}$ is positive as shown in Fig. 3.3. Therefore, $\Delta i_{-_{ba}}$ vs. $\Delta i_{-_{ab}}$ trajectory lies in second-quadrant (Q-2) of Δi-plane as shown in Fig. 3.4.

3.2.2 Negative Pole-to-ground fault (NGF)

The fault current seen by negative pole sensor at bus-a ($i^{F_2}_{-_{ab}}$) during NGF (F_2) can be obtained using (3.1). The direction of $i^{F_2}_{-_{ab}}$ will be from the fault site towards the buses due to the negative sign of the pole-to-ground voltage, as shown in Fig. 3.2(c). As a result, $\Delta i_{-_{ab}}$ for fault F_2 can be expressed as:

$$\Delta i^{F_2}_{-_{ab}}(t) = i^{F_2}_{-_{ab}}(t) - i^{pre}_{-_{ab}} \tag{3.6}$$

where $i^{pre}_{-_{ab}} = -i^{pre}_{+_{ab}}$ and, $i^{F_2}_{-_{ab}}$ is negative as shown in Fig. 3.5. Therefore, $\Delta i^{F_2}_{-_{ab}}$ is negative for F_2. Similarly at bus-b, $i^{pre}_{-_{ba}} = -i^{pre}_{+_{ba}}$ and $\Delta i_{-_{ba}}$ for fault F_2 is,

$$\Delta i^{F_2}_{-_{ba}}(t) = i^{F_2}_{-_{ba}}(t) - i^{pre}_{-_{ba}} \tag{3.7}$$

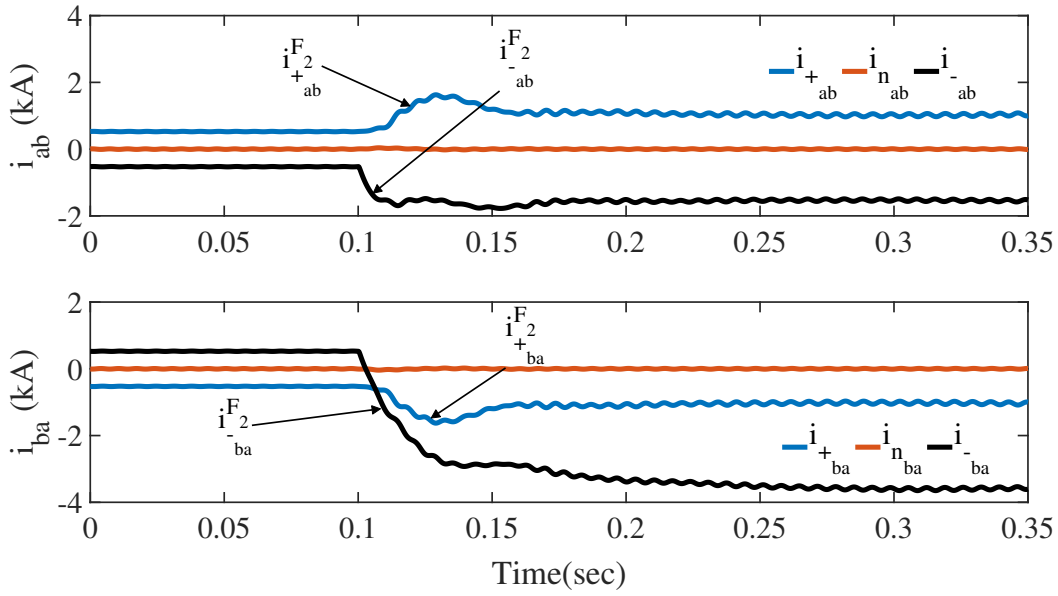


Figure 3.5: Pole domain currents at bus-a and bus-b during NGF (F_2).

Therefore, it is evident from Fig. 3.5 that $\Delta i_{-_{ba}}^{F_2}$ is negative for fault F_2 and the trajectory of $\Delta i_{-_{ba}}$ vs. $\Delta i_{-_{ab}}$ falls in third-quadrant (Q-3) of Δi-plane. However, the current measured by positive polarity sensors in the case of F_2 is $i_{+_{ba}}^{F_2} = -i_{+_{ab}}^{F_2}$ and, $\Delta i_{+_{ab}}$, $\Delta i_{+_{ba}}$ is given as,

$$\begin{aligned} \Delta i_{+_{ab}}^{F_2}(t) &= i_{+_{ab}}^{F_2}(t) - i_{+_{ab}}^{pre} \\ \Delta i_{+_{ba}}^{F_2}(t) &= -(i_{+_{ab}}^{F_2}(t) - i_{+_{ab}}^{pre}) \end{aligned} \tag{3.8}$$

from above it is clear that, $\Delta i_{+_{ab}}^{F_2}$ and, $\Delta i_{+_{ba}}^{F_2}$ are in opposition for fault F_2. From Fig. 3.5 it is clear that, $\Delta i_{+_{ab}}$ is positive in this case and $\Delta i_{+_{ab}}$ vs. $\Delta i_{+_{ba}}$ trajectory lies in the fourth-quadrant (Q-4) of Δi-plane as shown in Fig. 3.4. Therefore the selection of a proper condition for the generation of a trip signal is not possible using available Δi-plane [48] in this scenario.

The $\Delta i_{_{ab}}$ vs. $\Delta i_{_{ba}}$ trajectory plots for positive and negative-pole currents in the Δi-plane during various internal faults are shown in Fig. 3.4. By observing Fig. 3.4, it is found that for NGF, the Δi trajectory lies in the non-operating region of the Δi-plane proposed in [48]. Therefore, it is not possible to detect internal NGF using the method proposed in [48] in a bipolar DC microgrid.

A modified superimposed current-based unit protection strategy that utilizes the symmetrical component decomposition is proposed as a solution for bipolar DC systems.

3.3 Proposed Protection Method for Bipolar DC Microgrids

3.3.1 Fault detection

Occurrence of faults in the DC microgrid causes a high rate of change of current (ξ) [49]. However, under steady state, ξ is close to zero. Therefore ξ is considered as the criterion for triggering the main algorithm, which is given as

$$\xi = \frac{1}{N\Delta t}\left(\sum_{j=1}^{N} |i_{j+1} - i_j|\right) \tag{3.9}$$

where i_j is the current of j^{th} sample, Δt is the sampling interval, and N is the number of samples in a data window. When ξ exceeds the threshold (k), the protection starts. In this study, N = 10 for 20 kHz sampling frequency and $k = 6.2$ kA/sec.

3.3.2 Selection of Fault Zone

The selectivity in the proposed protection scheme is achieved by using symmetrical component decomposition of the bipolar DC system [116]. The measured pole domain currents are decomposed into the corresponding symmetrical components, which is given as

$$\begin{bmatrix} i_0 \\ i_1 \\ i_2 \end{bmatrix} = \frac{1}{\sqrt{6}} \begin{bmatrix} \sqrt{2} & \sqrt{2} & \sqrt{2} \\ 1 & -2 & 1 \\ \sqrt{3} & 0 & -\sqrt{3} \end{bmatrix} \begin{bmatrix} i_+ \\ i_n \\ i_- \end{bmatrix} \tag{3.10}$$

Here i_0, i_1, and i_2 are bias, unbalance, and balance components, respectively, in the symmetrical domain. i_+, i_n, and i_- are positive pole, neutral, and negative pole currents, respectively, in the pole domain. In the line section between buses a and b, the pole domain and the corresponding symmetrical domain currents are shown in Fig. 3.6. Being the system in balance condition i_0 and i_1 are zero and i_2 is non-zero, in the direction of i_+. The proposed analysis works to obtain the symmetrical domain currents for different fault situations using (3.10), and the relaying decision is obtained using (i_2) from both ends of the line segment.

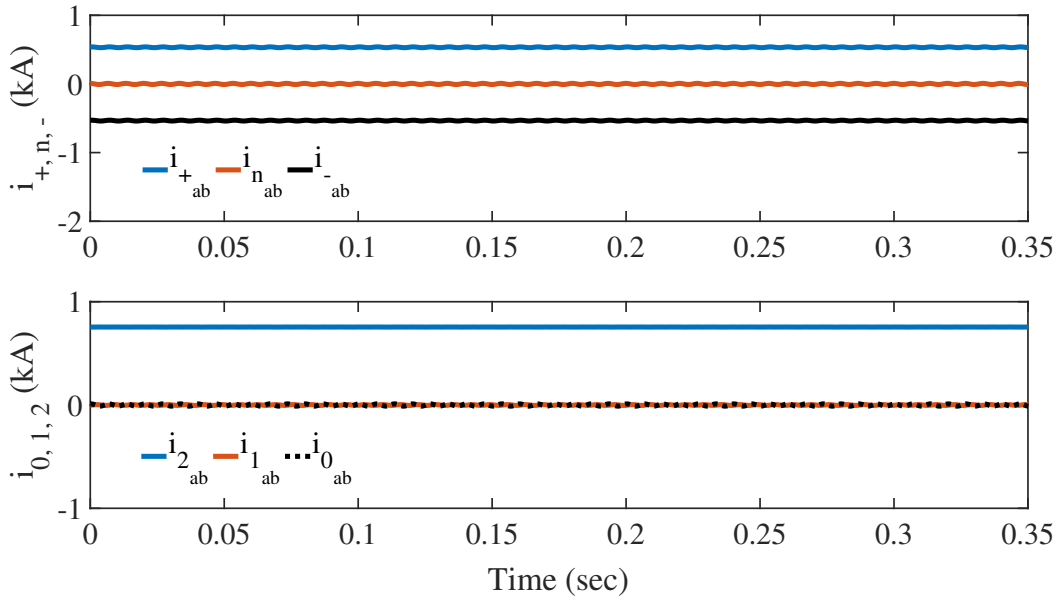


Figure 3.6: Pole domain and corresponding symmetrical domain currents from bus-a to bus-b.

3.3.3 Internal Faults

A generalized protection technique for three typical internal faults, namely PGF, NGF, and PPF, is discussed one by one.

3.3.3.1 Positive Pole to Ground Fault (PGF)

During internal PGF (F_1), $\Delta i_{+_{ab}}^{F_1}$ is positive using (3.2). $\Delta i_{-_{ab}}^{F_1}$ is given as,

$$\Delta i_{-_{ab}}^{F_1}(t) = i_{-_{ab}}^{F_1}(t) - i_{-_{ab}}^{pre} \tag{3.11}$$

Since $i_{-_{ab}}^{F_1}$ and $i_{-_{ab}}^{pre}$ are both in the same direction and negative as shown in Fig. 3.3, $\Delta i_{-_{ab}}^{F_1}$ is also negative (3.11). Therefore, the superimposed balance component at bus-a ($\Delta i_{2_{ab}}$) in case of F_1 is given as,

$$\Delta i_{2_{ab}}^{F_1}(t) = \frac{1}{\sqrt{2}}\left(\Delta i_{+_{ab}}^{F_1}(t) - (-\Delta i_{-_{ab}}^{F_1}(t))\right) \tag{3.12}$$

It is obvious from (3.11) and (3.12) that in case of F_1, $\Delta i_{2_{ab}}$ is positive. Similarly at bus-b, $\Delta i_{+_{ba}}^{F_1}$ is also positive, from (3.3). $\Delta i_{-_{ba}}^{F_1}$ is given as,

$$\Delta i_{-_{ba}}^{F_1}(t) = i_{-_{ba}}^{F_1}(t) - i_{-_{ba}}^{pre} \tag{3.13}$$

From Fig. 3.3 it is clear that, both $i_{-_{ba}}^{F_1}$ and $i_{-_{ba}}^{pre}$ are in same direction, and the value of fault current is more than pre-fault current, therefore, $\Delta i_{-_{ba}}^{F_1}$ is positive. However, in the

case of PGF, being the faulty pole, the change in the positive pole current is higher than that in the negative pole. Thus superimposed balance component at bus-b ($\Delta i_{2_{ba}}$) in case of F_1,

$$\Delta i_{2_{ba}}^{F_1}(t) = \frac{1}{\sqrt{2}}\left(\Delta i_{+_{ba}}^{F_1}(t) - (\Delta i_{-_{ba}}^{F_1}(t))\right) \tag{3.14}$$

is also positive.

3.3.3.2 Negative Pole to Ground Fault (NGF)

During an internal NGF (F_2), $\Delta i_{+_{ab}}^{F_2}$ is positive (3.8), whereas $\Delta i_{-_{ab}}^{F_2}$ is negative (3.6). Consequently $\Delta i_{2_{ab}}$ in case of F_2,

$$\Delta i_{2_{ab}}^{F_2}(t) = \frac{1}{\sqrt{2}}\left(\Delta i_{+_{ab}}^{F_2}(t) - (-\Delta i_{-_{ab}}^{F_2}(t))\right) \tag{3.15}$$

is positive. Similarly, at bus-b $\Delta i_{+_{ba}}^{F_2}$ is negative (3.8) and $\Delta i_{-_{ba}}^{F_2}$ is negative as well (3.7). However, being the faulty pole, magnitude of $\Delta i_{-_{ba}}^{F_2}$ is higher (Fig. 3.5). As a result, during F_2, the symmetrical domain superimposed current at bus-b ($\Delta i_{2_{ba}}$)

$$\Delta i_{2_{ba}}^{F_2}(t) = \frac{1}{\sqrt{2}}\left(-\Delta i_{+_{ba}}^{F_2}(t) - (-\Delta i_{-_{ba}}^{F_2}(t))\right) \tag{3.16}$$

is positive.

3.3.3.3 Pole-to-pole fault (PPF)

Consider a PPF (F_3) as shown in Fig. 3.2(a). The fault currents at both buses can be obtained by using (3.1) and are related as follows:

$$\begin{cases} i_{-_{ab}}^{F_3} = -i_{+_{ab}}^{F_3} \\ i_{-_{ba}}^{F_3} = -i_{+_{ba}}^{F_3} \end{cases} \tag{3.17}$$

The pole domain superimposed currents at bus-a and b will be,

$$\begin{cases} \Delta i_{+_{ab}}^{F_3}(t) = i_{+_{ab}}^{F_3}(t) - i_{+_{ab}}^{pre} \\ \Delta i_{-_{ab}}^{F_3}(t) = -(i_{+_{ab}}^{F_3}(t) - (i_{+_{ab}}^{pre})) \\ \Delta i_{+_{ba}}^{F_3}(t) = i_{+_{ba}}^{F_3}(t) - i_{+_{ba}}^{pre} \\ \Delta i_{-_{ba}}^{F_3}(t) = -(i_{+_{ba}}^{F_3}(t) - (i_{+_{ba}}^{pre})) \end{cases} \tag{3.18}$$

From (3.18), it is clear that $\Delta i_{+_{ab}}^{F_3}$ and $\Delta i_{-_{ab}}^{F_3}$ are in opposition. However, in the case of F_3, $\Delta i_{+_{ab}}^{F_3}$ is positive, as per the sign convention of the current, as shown in Fig. 3.2(a). Therefore, $\Delta i_{2_{ab}}$ in case of F_3,

$$\Delta i_{2_{ab}}^{F_3}(t) = \frac{1}{\sqrt{2}}\left(\Delta i_{+_{ab}}^{F_3}(t) - (-\Delta i_{-_{ab}}^{F_3}(t))\right) \tag{3.19}$$

is positive and, at bus-b

$$\Delta i_{2_{ba}}^{F_3}(t) = \frac{1}{\sqrt{2}}\left(\Delta i_{+_{ba}}^{F_3}(t) - (-\Delta i_{-_{ba}}^{F_3}(t))\right) \tag{3.20}$$

is also positive. Similarly during positive pole to neutral fault (F_4) and negative pole to neutral fault (F_5), $\Delta i_{2_{ab}}$ and $\Delta i_{2_{ba}}$ lies in first-quadrant of Δi-plane. From above, it is clear that during internal faults, Δi_2 at both local and remote ends lies in the first quadrant (Q-1) of Δi-plane.

3.3.4 External Faults

Consider the external fault F_6 in the line segment b-c as shown in 3.2(a). The pre and post-fault positive pole currents at bus-a and b are in opposition during F_6. Consequently, the positive pole superimposed current at both are,

$$\begin{cases} \Delta i_{+_{ab}}^{F_6}(t) = i_{+_{ab}}^{F_6}(t) - i_{+_{ab}}^{pre} \\ \Delta i_{+_{ba}}^{F_6}(t) = -(i_{+_{ab}}^{F_6}(t) - i_{+_{ab}}^{pre}) \end{cases} \tag{3.21}$$

From (3.21) and Fig. 3.2(a) it is clear that, the sign of $\Delta i_{+_{ab}}^{F_6}$ is positive and negative for $\Delta i_{+_{ba}}^{F_6}$. Similarly, the negative pole current seen at bus-a, $i_{-_{ab}}^{F_6} = -i_{+_{ab}}^{F_6}$ and, the negative-pole superimposed current at both ends of the line segment during external fault F_6 are

$$\begin{cases} \Delta i_{-_{ab}}^{F_6}(t) = i_{-_{ab}}^{F_6}(t) - i_{-_{ab}}^{pre} \\ \Delta i_{-_{ba}}^{F_6}(t) = -(i_{-_{ab}}^{F_6}(t) - i_{-_{ab}}^{pre}) \end{cases} \tag{3.22}$$

Therefore $\Delta i_{-_{ab}}^{F_6}$ is negative, and $\Delta i_{-_{ba}}^{F_6}$ is positive in case of external fault F_6. Therefore Δi_2 between the line segment are given as,

$$\begin{cases} \Delta i_{2_{ab}}^{F_6}(t) = \frac{1}{\sqrt{2}}\left(\Delta i_{+_{ab}}^{F_6}(t) - (-\Delta i_{-_{ab}}^{F_6}(t))\right) \\ \Delta i_{2_{ba}}^{F_6}(t) = \frac{1}{\sqrt{2}}\left(-\Delta i_{+_{ab}}^{F_6}(t) - \Delta i_{-_{ab}}^{F_6}(t)\right) \end{cases} \tag{3.23}$$

Table 3.2: Superimposed fault current (symmetrical domain) trajectories for different types of faults.

Faults	Internal Fault		External Fault (F_6)		External Fault (F_7)	
	Δi_2	Δi_1	Δi_2	Δi_1	Δi_2	Δi_1
PGF	Q-1	Q-1	Q-4	Q-4	Q-2	Q-2
NGF	Q-1	Q-3	Q-4	Q-2	Q-2	Q-4
PPF	Q-1	Origin	Q-4	Origin	Q-2	Origin

It can be concluded that during F_6, $\Delta i_{2_{ab}}^{F_6}$ and $\Delta i_{2_{ba}}^{F_6}$ are in opposition, and, $\Delta i_{2_{ab}}^{F_6}$ vs. $\Delta i_{2_{ba}}^{F_6}$ plot lies in fourth quadrant of Δi-plane. Similarly, for external fault, F_7, the direction of currents are opposite to that in F_6, and the symmetrical domain superimposed currents between line segment are,

$$\begin{cases} \Delta i_{2_{ab}}^{F_7}(t) = \dfrac{1}{\sqrt{2}}\left(-\Delta i_{+_{ab}}^{F_6}(t) - \Delta i_{-_{ab}}^{F_6}(t)\right) \\ \Delta i_{2_{ba}}^{F_7}(t) = \dfrac{1}{\sqrt{2}}\left(\Delta i_{+_{ab}}^{F_6}(t) - (-\Delta i_{-_{ab}}^{F_6}(t))\right) \end{cases} \tag{3.24}$$

So, in case of external fault F_7, $\Delta i_{2_{ab}}^{F_7}$ is negative and $\Delta i_{2_{ba}}^{F_7}$ is positive and $\Delta i_{2_{ab}}^{F_7}$ vs. $\Delta i_{2_{ba}}^{F_7}$ plot lies in second quadrant of Δi-plane.

3.4 Fault Type Classification

A bipolar DC system with a metallic return offers the key advantage of maintaining supply continuity even when a PGF occurs. This inherent redundancy enhances the reliability of the system, especially in critical applications. However, to ensure safe and effective operation, it becomes essential to accurately identify the faulty pole in the event of an internal fault.

Once an internal fault is detected, the identification process is carried out by analyzing the unbalanced component of the currents, which is derived solely from local current measurements. The unbalance component in the symmetrical domain is given in (3.10) as,

$$i_{1_{ab}}(t) = \frac{1}{\sqrt{6}}\left(i_{+_{ab}}(t) - 2i_{n_{ab}}(t) + i_{-_{ab}}(t)\right) \tag{3.25}$$

and the unbalance superimposed component at bus-a is,

$$\Delta i_{1_{ab}} = \frac{1}{\sqrt{6}} \left(\Delta i_{+_{ab}} - 2\Delta i_{n_{ab}} + \Delta i_{-_{ab}} \right) \tag{3.26}$$

For internal fault F_1, $\Delta i_{+_{ab}}$ and $\Delta i_{-_{ab}}$ both are positive and neutral current will be zero as shown in Fig. 3.3. Therefore, $\Delta i_{1_{ab}}$ will be positive for fault F_1. However in case of positive-pole to neutral short circuit (F_4) the current flowing through the neutral at bus-a ($i_{n_{ab}}$) will be in opposition to that of $i_{+_{ab}}$ thus, $\Delta i_{n_{ab}}$ is negative, resulting in $\Delta i_{1_{ab}}$ to become positive (3.26). Similarly, in case of negative pole fault $\Delta i_{1_{ab}}$ will be negative, and for balance fault, it will be zero as given in Table 3.2. Q-1, Q-2, Q-3, and Q-4 in Table 3.2 are the quadrants of Δi-plane (Fig. 3.4). Similar calculations at bus-b give $\Delta i_{1_{ba}}$ positive for PGF, negative for NGF, and zero for PPF. In this way, the fault type can be identified, and consequently, the corresponding pole(s) can be isolated, and the healthy pole can maintain the continuity of supply with reduced capacity. A threshold (i_{th}) near the origin is selected to improve the security of the protection operation against measurement error using Δi-plane. The value of i_{th} is selected as 1% of the pre-fault current [117].

3.5 Resiliency of the Proposed Method Against Cyber Attack

Resiliency analysis is crucial in communication-assisted protection schemes (unit protection in this case) for DC microgrids as it ensures reliable and secure fault detection even under adverse conditions such as communication failures, cyberattacks, or system disturbances. Since these protection schemes rely heavily on timely data exchange between the two ends of the protected line segment, resiliency analysis helps identify vulnerabilities and supports the design of fault-tolerant and redundant architectures. It ensures the system can maintain stability, isolate faults promptly, and continue operating safely despite disruptions. Additionally, it plays a key role in meeting safety standards and enhancing the overall robustness of protection strategies in modern, communication-dependent DC microgrid environments.

The performance of the proposed technique is analyzed to ascertain whether the system is subjected to internal faults, a cyber attack, or external faults. No trip signal is

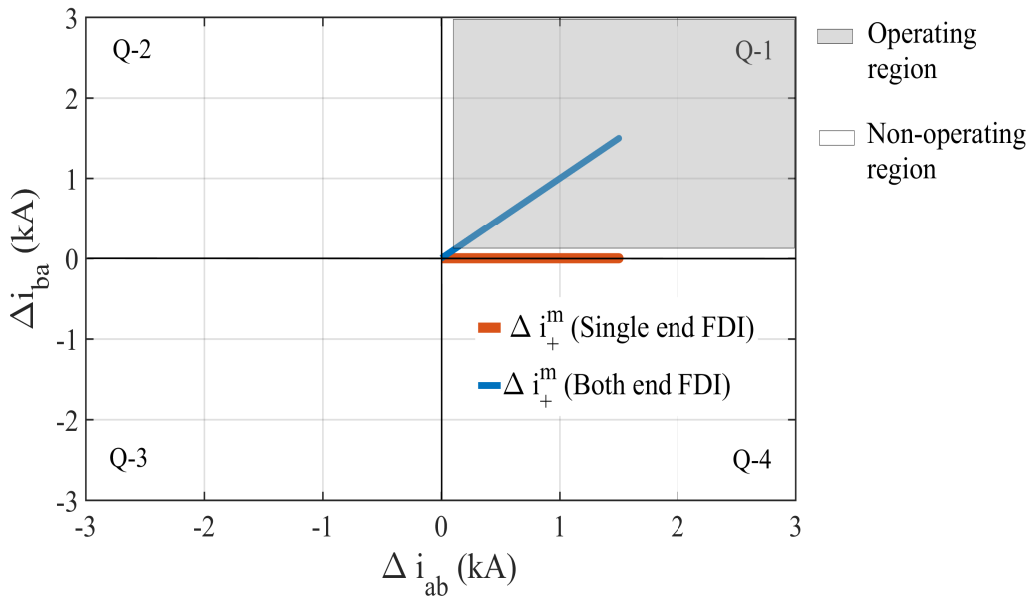


Figure 3.7: Pole domain superimposed currents in Δi-plane for FDI attacks.

produced when an external fault or cyber attack occurs.

3.5.1 Resiliency Against False Data Injection (FDI)

FDI attacks can significantly impact the performance of unit protection schemes in DC microgrids by manipulating measurement data such as current or voltage values. These attacks can lead to incorrect fault detection, either missing real faults or falsely identifying healthy conditions as faults, resulting in delayed or unnecessary tripping. Since unit protection relies on accurate and timely data from multiple points in the system, FDI attacks can disrupt coordination between relays, reduce protection reliability, and compromise system stability. Ultimately, this poses serious risks to equipment safety and power continuity, highlighting the need for secure and resilient communication channels in DC microgrid protection systems.

Despite the vulnerability of communication-based protection schemes to cyber attacks, the superimposed current-based protection scheme [48] is inherently resistant to FDIs at a single end. The available differential protection scheme is prone to FDIs even in case of single-end attack [61].

Consider an FDI attack in which $i_{+_{ab}}$ is manipulated by the attacker. The manipulated value $i^m_{+_{ab}} = i_{+_{ab}} + \phi$ is received at the IED. Where ϕ is the difference between $i^m_{+_{ab}}$

and $i_{+_{ab}}$. $\Delta i_{+_{ab}}$ in case of FDI is,

$$\Delta i^{m}_{+_{ab}} = i^{m}_{+_{ab}} - i^{pre}_{+_{ab}} \tag{3.27}$$

Depending on ϕ, $\Delta i^{m}_{+_{ab}}$ can be positive or negative. Therefore, the method in [48] may malfunction due to an FDI attack at both ends for positive superimposed current. It is clear from Fig. 3.7 that, for a single-end attack, the trajectory lies on the non-operating region, whereas for the attack on both ends, it falls on the operating region, which leads to the false operation of the protection function.

In symmetrical domain, $\Delta i_{2_{ab}}$ during FDI using (3.10) is given as,

$$\Delta i^{m}_{2_{ab}}(t) = \frac{1}{\sqrt{2}}\left(\Delta i^{m}_{+_{ab}}(t) - (\Delta i_{-_{ab}}(t))\right) \tag{3.28}$$

Here $\Delta i_{-_{ab}}$ will be zero, as the manipulation in $i_{+_{ab}}$ will not affect $i_{-_{ab}}$. Thus, for positive $\Delta i^{m}_{+_{ab}}$, the value of $\Delta i^{m}_{2_{ab}}$ is also positive. Similarly, FDI at the remote end cause $\Delta i_{2_{ba}}$ to become positive.

Now, consider the case of FDI in the negative pole quantity at bus-a. The modified negative pole current $i^{m}_{-_{ab}} = i_{-_{ab}} + \phi$ and change in negative pole current $\Delta i^{m}_{-_{ab}} = i^{m}_{-_{ab}} - i^{pre}_{-_{ab}}$. $\Delta i_{2_{ab}}$ in this instance is given as,

$$\Delta i^{m}_{2_{ab}}(t) = \frac{1}{\sqrt{2}}\left(\Delta i_{+_{ab}}(t) - (\Delta i^{m}_{-_{ab}}(t))\right) \tag{3.29}$$

it is obvious from (3.29) that, the negative value of $\Delta i^{m}_{-_{ab}}$ causes the value of $\Delta i_{2_{ab}}$ to become positive. A simultaneous attack at the remote end may cause $\Delta i_{2_{ba}}$ also to become positive, resulting in a false operation.

To prevent the false operation of the IED due to an FDI attack, the proposed method will first check the condition of the FDI attacks, which is derived by computing the superimposed bias component (Δi_0) at both ends. Δi_0 at bus-a is given as,

$$\Delta i_{0_{ab}} = \frac{1}{\sqrt{3}}\left(\Delta i_{+_{ab}} + \Delta i_{n_{ab}} + \Delta i_{-_{ab}}\right) \tag{3.30}$$

Since i_0 is zero during normal operating conditions, thus it is clear from (3.30) that any change in either of the single pole measurement data will be directly reflected in $\Delta i_{0_{ab}}$.

If the false data is injected in positive-pole sensors at both ends, then

$$\begin{cases} \sqrt{3}\Delta i_{0_{ab}} = \Delta i_{+_{ab}} \\ \sqrt{3}\Delta i_{0_{ba}} = \Delta i_{+_{ba}} \end{cases} \tag{3.31}$$

similarly, if there is manipulation in negative pole measurement data at both ends,

$$\begin{cases} \sqrt{3}\Delta i_{0_{ab}} = \Delta i_{-_{ab}} \\ \sqrt{3}\Delta i_{0_{ba}} = \Delta i_{-_{ba}} \end{cases} \tag{3.32}$$

Any FDI that happens in the corresponding line satisfies one of the four circumstances listed in (3.31) and (3.32), and in that scenario, the protection system will not operate.

3.5.2 Resiliency Against Time Synchronization Attack (TSA)

It is possible to interfere with the synchronism of line current data by spoofing the IEEE 1588 Precision Timing Protocol at a substation [118]. TSA can operate the line current differential relay even during normal power transients in the system [25]. However, the proposed method is resilient to TSA.

Assuming the TSA changes the time-stamped samples of the remote end currents by nT_s samples leading or lagging. In this case, $i_{2_{ba}}(k) = i_{2_{ba}}(k \pm n)$ and, due to the normal power transient during TSA, $\Delta i_{2_{ab}}$ may become positive. However, because of TSA at the remote end, the change in $i_{2_{ba}}$ due to power transient will be delayed, and $\Delta i_{2_{ba}}$ remains zero and relay will not operate due to TSA. The simulation results in section 3.6.5 verify it. The flow chart of the proposed method is shown in Fig. 3.8.

3.6 Performance Evaluation

The performance of the proposed method is validated on the test system shown in Fig. 3.1, which is simulated using RTDS available in the existing smart grid laboratory in our institute (Fig. 3.9). Data are extracted with the sampling frequency (f_s) of 20 kHz, and the fault inception time is 0.1 sec for all fault cases.

3.6.1 Performance for Different Internal Faults

3.6.1.1 Validation for PGF

A PGF (F_1 in Fig. 3.2(a)) is simulated in the middle of the line segment a-b with a fault resistance $R_f = 0.1\ \Omega$. The simulation results in Fig. 3.10(a) shows that before fault, $i_{2_{ab}}$ and $i_{2_{ba}}$ are in opposition, while during fault the direction of $i_{2_{ba}}$ gets reverse. Therefore

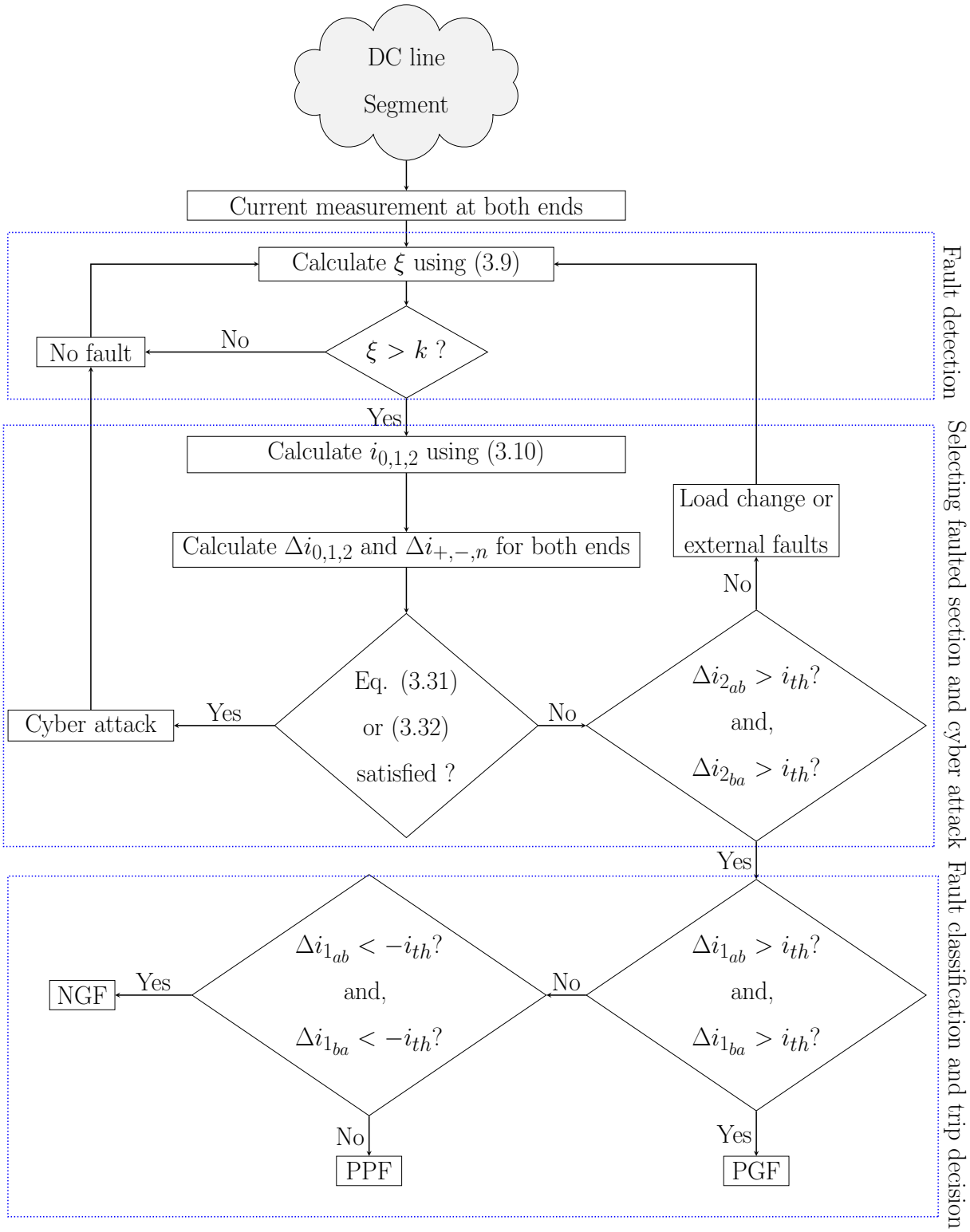


Figure 3.8: Flow chart of the proposed method.

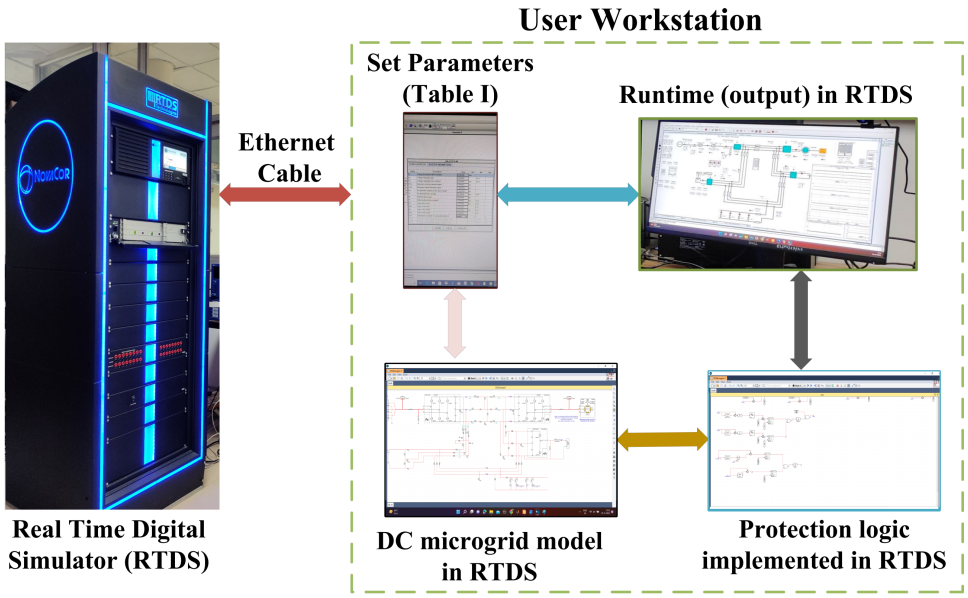


Figure 3.9: Real-time digital simulation platform.

$\Delta i_{2_{ab}}$ and $\Delta i_{2_{ba}}$ are both positive. Furthermore, $\Delta i_{1_{ab}}$ and $\Delta i_{1_{ba}}$ are also positive, which confirms that the positive pole is involved in the fault. The performance is also validated for a short circuit between the positive pole and the neutral conductor (F_4 in Fig. 3.2(a)), and the simulation results are shown in Fig. 3.10(b).

3.6.1.2 Validation for NGF

An NGF (F_2 in Fig. 3.2(a)) is simulated in the line segment between bus-a and bus-b as in the PGF case. The decisive parameters are obtained in Fig. 3.10(c), which clarifies the effectiveness of the proposed scheme for fault F_2. Fig. 3.9(d) analyzes the decision variable for the negative pole to neutral short circuit (F_5 in Fig. 3.2(a)). It is clear from Fig. 3.10(c) and (d) that, both $\Delta i_{2_{ab}}$ and $\Delta i_{2_{ba}}$ are positive and, $\Delta i_{1_{ab}}$, $\Delta i_{1_{ba}}$ are negative. Thus, the fault can be classified as internal NGF.

3.6.1.3 Validation for pole-to-pole fault (PPF)

Fig. 3.10(e) shows the fault identification for PPF (F_3). $\Delta i_{2_{ab}}$ and $\Delta i_{2_{ba}}$ both are positive for pole-to-pole fault, and i_1 is constant at both bus-a and bus-b as evident from Fig. 3.10(e) and hence $\Delta i_{1_{ab}}$, $\Delta i_{1_{ba}}$ are zero in this case. Therefore, internal PPF can be confirmed.

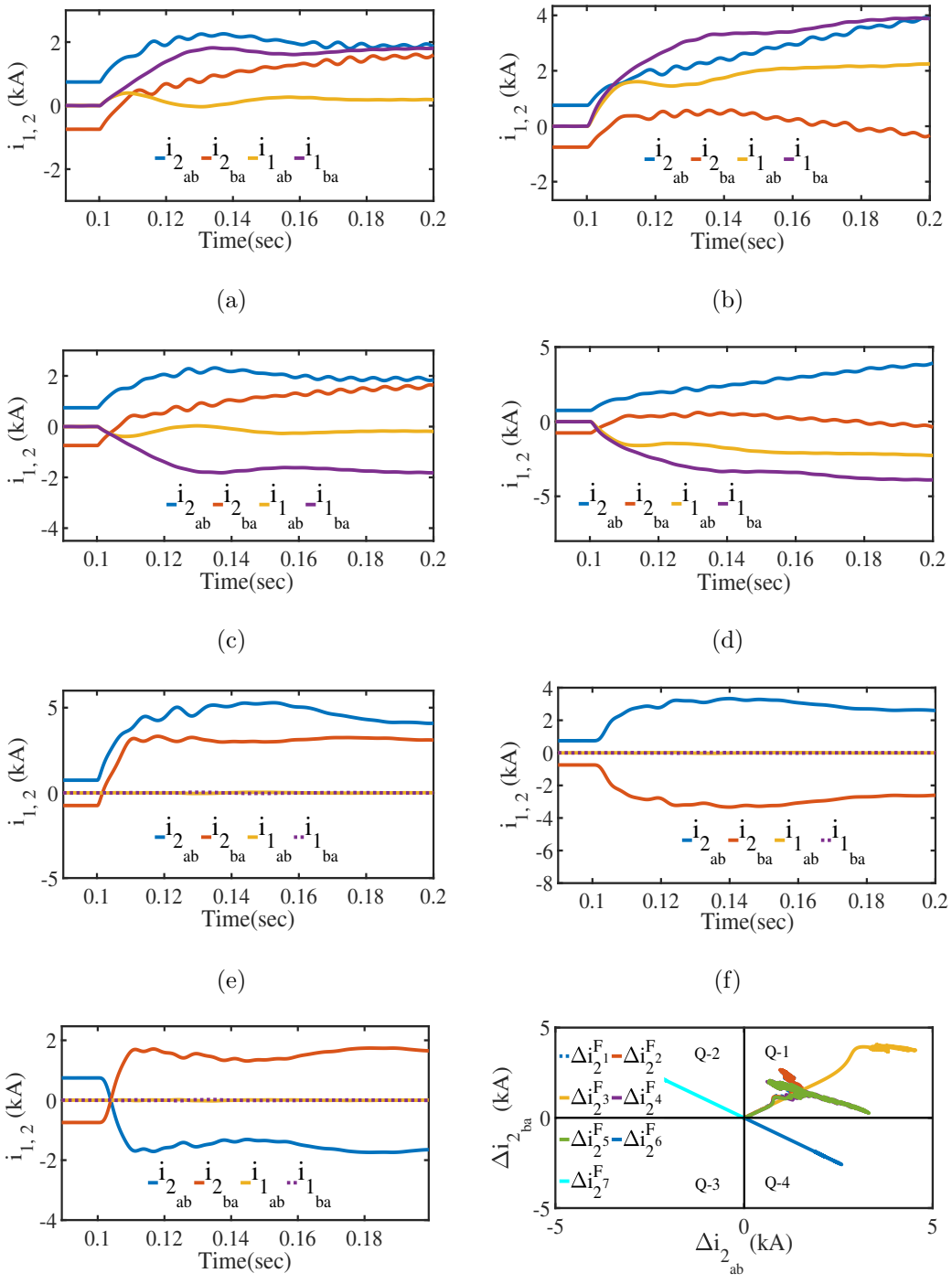
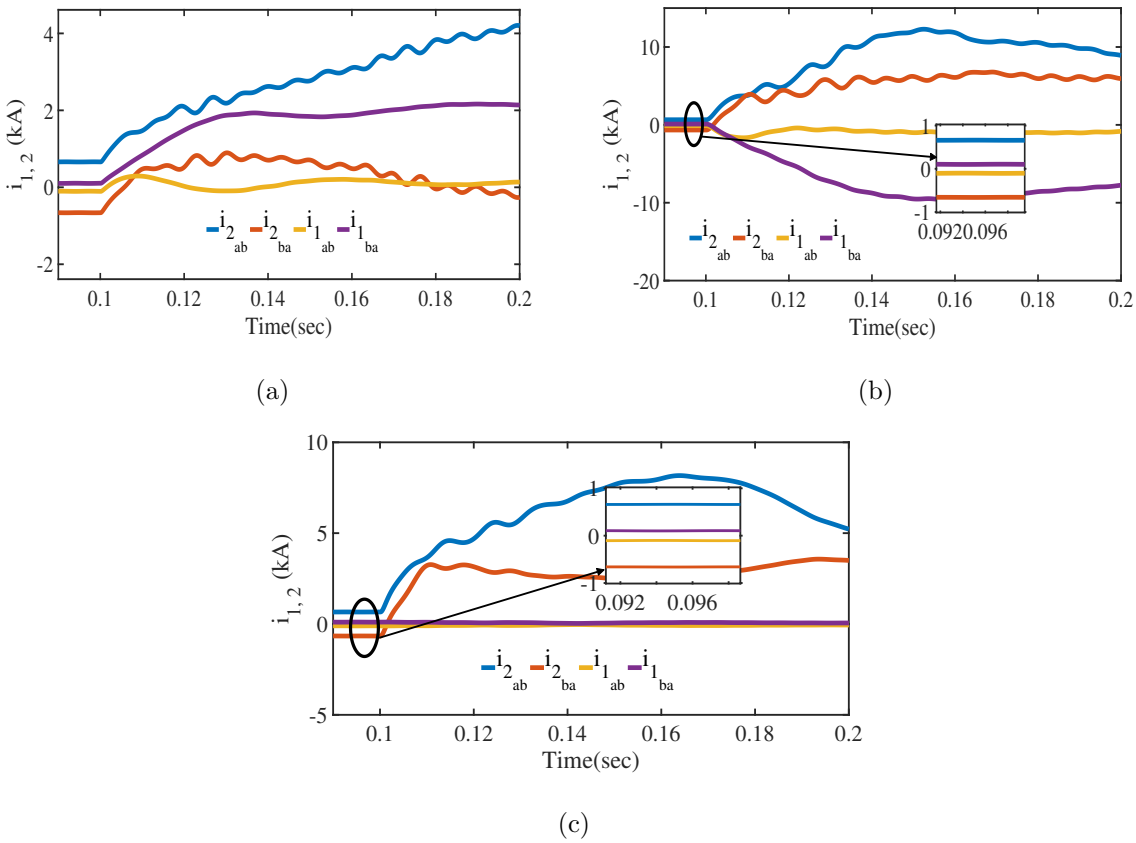


Figure 3.10: Balance and unbalance components for (a) fault F_1 (b) fault F_4 (c) fault F_2 (d) fault F_5 (e) fault F_3 (f) external fault (F_6) (g) external fault (F_7) and, (h) Δi_2 in Δi-plane for internal and external faults.



(a) (b)

(c)

Figure 3.11: Balance and unbalance currents during unbalance loading for (a) fault F_1 (b) fault F_2 (c) fault F_3.

3.6.2 Performance for External Faults

Simulation results given in Fig. 3.10(f) and 3.10(g) analyze the decision parameters for external faults F_6 and F_7, respectively. Fig. 3.10(f) shows that for F_6, $\Delta i_{2_{ab}}$ is positive and $\Delta i_{2_{ba}}$ is negative. Similarly for F_7, $\Delta i_{2_{ab}}$ is negative and $\Delta i_{2_{ba}}$ is positive. Fig. 3.10(h) represents the trajectories of superimposed currents $\Delta i_{2_{ab}}$ and $\Delta i_{2_{ba}}$ in Δi-plane, for different internal and external faults. It is clear from Fig. 3.10(h) that, the proposed method can efficiently distinguished the internal and external faults.

3.6.3 Performance During Unbalance Loading

Bipolar DC system has the possibility of unbalancing, therefore, it is necessary to validate the performance of the proposed method when different loads are connected to the two poles of the bipolar DC bus.

A resistive load of 100 kW is connected at the positive pole of bus-a, which results in

Table 3.3: Pre and post-pault symmetrical domain currents for internal faults during unbalanced loading.

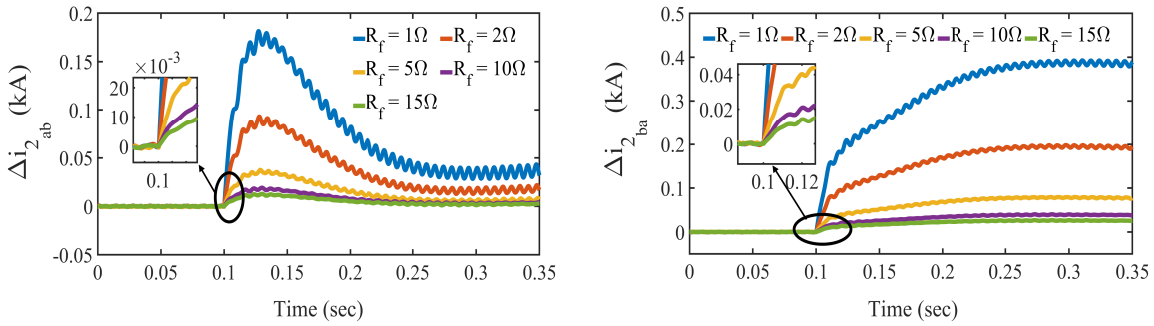
Currents (A)		Pre-fault	Post Fault (at t=0.101 sec)		
			F_1	F_2	F_3
Bus-a	$i_{1_{ab}}$	-101	-42.8	-237.5	-101
	$i_{2_{ab}}$	661	769	898.6	1017.6
	$\Delta i_{1_{ab}}$	–	58.2	-136.5	0
	$\Delta i_{2_{ab}}$	–	108	237.6	356.6
Bus-b	$i_{1_{ba}}$	101	169.3	-36	101
	$i_{2_{ba}}$	-661	-549.7	-425	-303.9
	$\Delta i_{1_{ba}}$	–	68.3	-137	0
	$\Delta i_{2_{ba}}$	–	111.3	236	357.1

the unsymmetrical current distribution in the line segment connecting bus-a and bus-b. Fig. 3.11(a), 3.11(b), and 3.11(c) analyze Δi_1 and Δi_2 at both buses for internal faults F_1, F_2, and F_3 respectively. The nonzero value of the pre-fault unbalanced component at both buses revealed the condition of non-symmetrical line loading, as shown in Fig. 3.11. Further, post-fault values of $i_{2_{ab}}$ and $i_{2_{ba}}$ start moving in a positive direction after the inception of fault in all three fault conditions F_1, F_2, and F_3 and therefore, $\Delta i_{2_{ab}}$ and $\Delta i_{2_{ba}}$ are positive. Table 3.3 shows the pre and post-fault symmetrical domain currents during internal faults in the case of unbalanced loading.

3.6.4 Effect of Fault Resistance

Fault resistance significantly affects the performance of protection systems in DC microgrids. Low-resistance faults produce high fault currents that are easily detected by conventional overcurrent-based protection methods. However, high-resistance faults generate lower fault currents that may not exceed detection thresholds, leading to delayed or missed fault identification. Thus, it is required to validate the performance of the proposed method with variations in fault resistance during internal faults.

Fault resistance DC cable varying from 0 to 0.5 Ω for short circuit faults [44, 49]. However, it may go beyond this level for ground faults depending on the object's resistance



(a) (b)

Figure 3.12: Effect of fault resistance on Δi_2 at (a) bus-a and,(b) bus-b.

Table 3.4: Δi_2 at 10^{th} sample after threshold crossing.

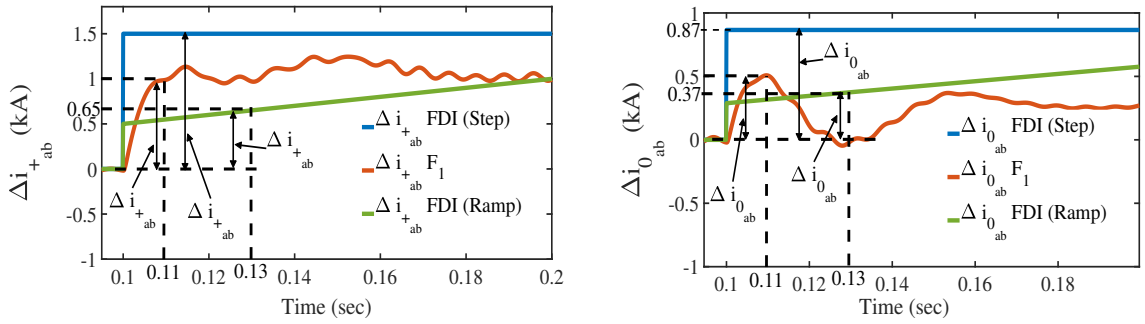
R_f (Ω)	$\Delta i_{2_{ab}}$	$\Delta i_{2_{ba}}$
1	18.4 A	17.13 A
2	12.5 A	12.4 A
5	9.29 A	9.53 A
10	7.96 A	8.4 A
15	7.83 A	7.91 A

in the fault path. Therefore, for validating the performance of the proposed method under high resistance fault, internal PGF with different fault resistances ranging from 1 to 15 Ω are simulated. The simulation results consist of Δi_2 at bus-a and bus-b are shown in Fig. 3.12(a) and 3.12(b), respectively. It is clear from Fig. 3.12 that $\Delta i_{2_{ab}}$ and $\Delta i_{2_{ba}}$ both are positive even for high resistance fault. Table 3.4 represents the values of $\Delta i_{2_{ab}}$, and $\Delta i_{2_{ba}}$ at the instant of 10^{th} sample from the instant of threshold (i_{th}= 7.5 A in this case) crossing, for different fault resistance.

3.6.5 Performance Against Cyber Attacks

3.6.5.1 Validation Against FDI Attack

Fig. 3.13 shows the simulation results for the FDI attack. A step signal of amplitude 1.5 is added at 0.1 sec to both ends of the positive pole measurement that results in the violation of threshold ($\xi > k$), and the relaying operation starts. However, either of the conditions specified in (3.31) or (3.32) is satisfied in this case, and the relay is prevented



(a) (b)

Figure 3.13: Simulation results for FDI attack.

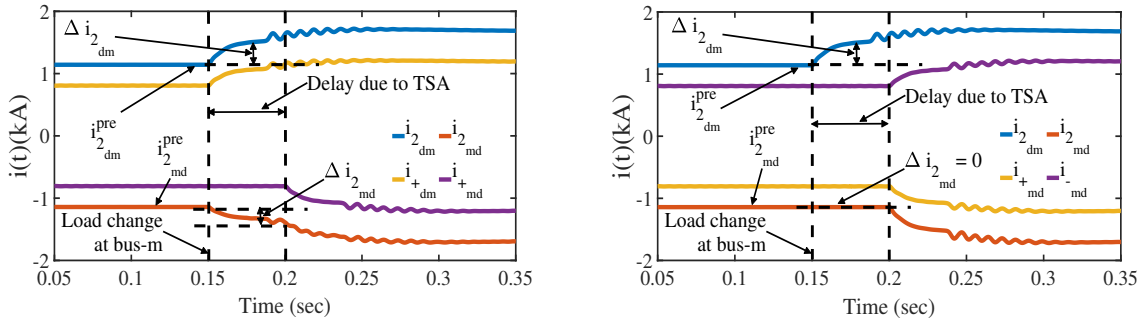
from maloperation. Similarly, the performance is also verified for a ramp signal having a slope of 5 units, and the simulation results confirm that for any change in positive pole measurement data, the same change is reflected in the bias component current at the corresponding end, and the relay can be prevented from the false operation.

3.6.5.2 Validation Against TSA

A TSA occurs at the positive pole between bus-d and bus-m, where $i_{+_{md}}$ is the parameter under synchronization attack. For a load change at 0.15 sec at bus-m, the positive pole current $i_{+_{dm}}$ increases, and $\Delta i_{+_{dm}}$ becomes positive, causing $\Delta i_{2_{dm}}$ to become positive, whereas, at the same instant due to the TSA, $i_{+_{md}}$ does not change and $\Delta i_{+_{md}}$ is zero. However, due to a change in negative pole current, $\Delta i_{2_{md}}$ is not zero, and it becomes negative, as shown in Fig. 3.14(a). Similarly, if the TSA affects both pole current data from bus-m, then $\Delta i_{2_{md}}$ becomes zero for the delay interval (0.05 sec in this case) as shown in Fig. 3.14(b), and therefore, the trajectory of $\Delta i_{2_{dm}}$ vs. $\Delta i_{2_{md}}$ coincides with the positive $\Delta i_{2_{dm}}$ axis, which is the non-operating region.

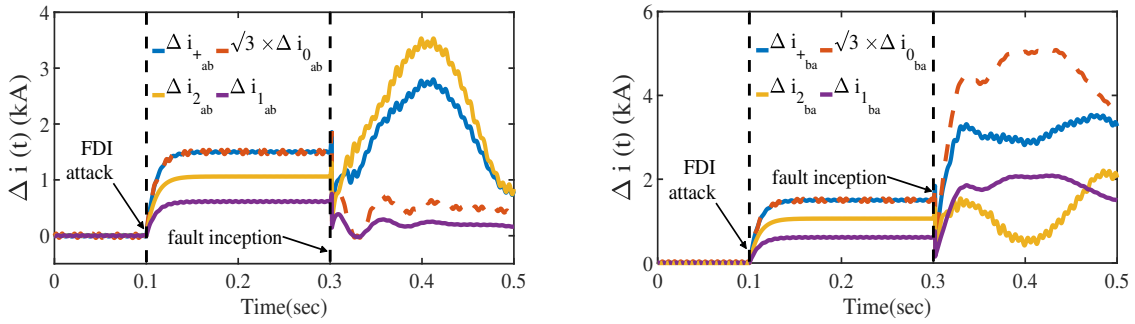
3.6.6 Validation for simultaneous faults and cyber attack

The performance of the proposed scheme is validated when a fault and a cyber attack occur simultaneously. FDI and TSA are simulated simultaneously with the fault and discussed one by one.



(a) (b)

Figure 3.14: Simulation results for TSA (a) at positive pole (b) at both positive and negative pole.

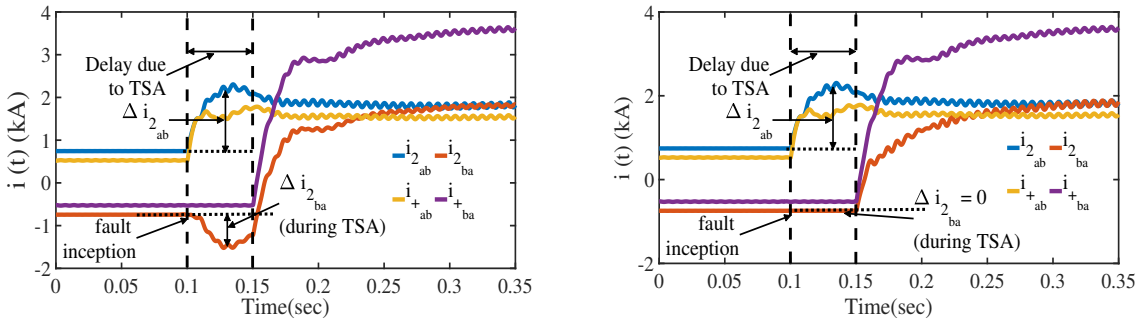


(a) (b)

Figure 3.15: Simulation results for internal fault simultaneous to FDI attack (a) response at bus-a (b) response at bus-b.

3.6.6.1 Faults Simultaneous to FDI Attack

An FDI attack is simulated at both bus-a and bus-b at 0.1 sec by adding a step signal of amplitude 1.5 units to the currents $i_{+_{ab}}$ and $i_{+_{ba}}$. During the FDI attack, an internal PGF (F_1) occurs at 0.3 sec. From simulation results in Fig. 3.15, it is clear that during the FDI attack (from 0.1 sec to 0.3 sec), (3.31) satisfies, and the situation is detected as an FDI attack. However, after fault inception, (3.31) violates, and the values of $\Delta i_{2_{ab}}$ and $\Delta i_{2_{ba}}$ both are positive; further, $\Delta i_{1_{ab}}$ and $\Delta i_{1_{ba}}$ are also positive, as shown in Fig. 3.15(a) and 3.15(b), respectively, and internal PGF is detected.



(a) (b)

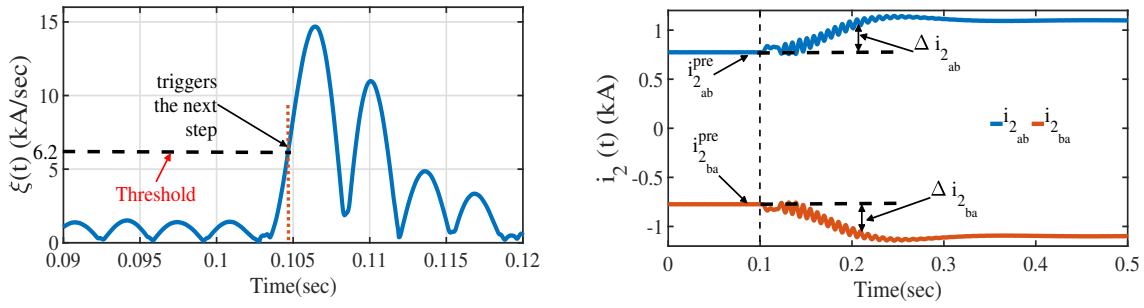
Figure 3.16: Simulation results for internal fault simultaneous to TSA (a) TSA in i_{+ba} (b) TSA in both i_{+ba} and i_{-ba}.

3.6.6.2 Faults Simultaneous to TSA

An internal PGF (F_1) takes place at 0.1 sec simultaneous to TSA at bus-b, where i_{+ba} and i_{-ba} are the parameters under synchronization attack. As shown in Fig. 3.16(a), for an internal fault occurring simultaneous to TSA in i_{+ba}, $\Delta i_{2_{ba}}$ is negative due to the delay caused by TSA. In this case, the relay is not able to detect internal faults quickly. Further Fig. 3.16(b) shows the simulation results for internal fault when both i_{+ba} and i_{-ba} are under TSA. In this case, $\Delta i_{2_{ba}}$ becomes zero, and the relay fails to detect the internal fault quickly. The relay response delay is equal to the TSA-introduced delay (0.05 sec in this case), as shown in Fig. 3.16. Although this will be the worst situation, backup protection will be required to protect the system under such circumstances.

3.6.7 Robustness of the Proposed Method Against Power Transients

To validate the performance of the proposed method against power transients, a load of 1.5 MW is disconnected at 0.1 sec from the load bank at bus-m. As evident in Fig. 3.17(a), due to sudden load change, ξ exceeds the threshold and triggers the next step of protection. $i_{2_{ab}}$ increases, whereas $i_{2_{ba}}$ decreases, as shown in Fig. 3.17(b). Therefore, $\Delta i_{2_{ab}}$ becomes positive and $\Delta i_{2_{ba}}$ is negative, and the relay will not operate. This shows that the proposed protection scheme is not affected by current fluctuations due to changes in system power.



(a) (b)

Figure 3.17: Effect of power transients on proposed method (a) ξ (b) i_2.

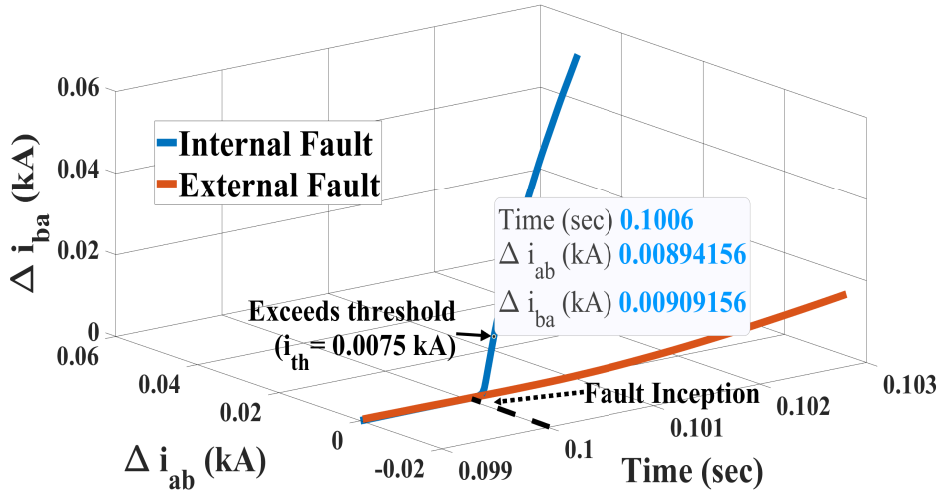


Figure 3.18: Operating time for the proposed scheme.

3.6.8 Protection Decision Time

A PGF with a fault resistance of 1 Ω is simulated in the middle of line sections a-b (internal fault) and b-c (external fault). As shown in Fig. 3.18, the Δi_2 trajectory for internal fault exceeds the threshold (i_{th}) within 0.6 msec after the inception of fault. Therefore, the fault detection time in this case is 0.6 msec. However, with different fault resistances, the operating time may vary due to variations in the time constant of the fault loop. The operating time for maximum fault resistance considered in this work (15 Ω) is 10 msec. Considering the higher rate of rise of current in DC microgrids and the availability of fast-acting DC circuit breakers, the protection decision time for such systems should be in the range of 1 to 2 msec [33, 104].

Table 3.5: Comparison with various fault detection methods.

Parameters/Features	**Proposed method**	**Available methods**			
		[14]	**[25]**	**[43]**	**[61]**
Resiliency towards false data injection attack	Yes	-	Yes	-	Yes
Resiliency towards time synchronization attack	Yes	-	Yes	Yes	Yes
Fault type classification	Yes	-	Yes	-	Yes
Signal required	Only I	V and I	V and I	Only I	V and I
CLR/ Any Extra arrangement required	No	Yes	Yes	No	Yes
Selectivity for high resistance fault	High	Low	Low	High	Low

3.7 Comparison with Available Methods

Table 3.5 shows the comparison of the proposed method with other available methods [14], [25], [43], and [61]. As observed from Table 3.5, the proposed method only uses line currents to provide cyber resilient protection, in contrast to the methods available [25], [43], and [61] that use both voltage and currents. Compared to the technique proposed in [14],[43], the proposed method also provides fault type classification, which is important for bipolar DC microgrids for achieving the highest selectivity. The proposed method does not require any extra arrangements, such as CLR or POC, as compared to [14], [25], and [61]. Further, the selectivity of these methods deteriorates with high fault resistance, whereas the proposed method provides high selectivity for high resistance faults. All the aforementioned points clearly indicate the superiority of the proposed method compared to other available methods.

3.8 Discussion

The proposed protection method requires only a current sensor at both ends and one IED in each section. Therefore, it provides an economical, and computationally efficient (only change in current) solution for fault detection, fault type classification, and cyber attack

distinction in a bipolar DC microgrids. The main strength of the proposed method is its inherent resiliency to single-end cyber attacks in contrast to conventional differential protection. Further, both ends attack, and multiple sensors attack at a single end can be correctly identified using the proposed scheme. However, in case of internal fault during TSA, the response of the proposed method is delayed (the same as the delay introduced by TSA) and, therefore, it does not detect the internal fault instantly. To make the system more resilient, a temper proof communication medium is required. One of the secure communication is considered and discussed in the next chapter. The performance of the proposed method is also validated on large system and discussed in Appendix A.

3.9 Summary

A cyber-resilient protection scheme is proposed for bipolar DC microgrids. The symmetrical component decomposition of the pole currents provides a useful perspective to identify and classify the internal faults. The trajectories of superimposed component of balanced component at both ends on first quadrant of the Δi-plane confirms the internal faults and that on other quadrants reveals non-fault situations including cyber attacks. In contrast with the previous research, the proposed method only requires line current information for identifying faults and cyber attacks. The proposed scheme is easy to implement and is inherently resilient to single-end attacks when compared to the available current differential techniques. The method is found to be effective for detecting high-resistance faults. Simulation results using data obtained from RTDS verify the efficacy and robustness of the proposed method for different cases including faults and cyber attacks and are found to be accurate.