Technical Report

Title: Formal Specifications and Verification of MAS-Based Protection Systems Using Probabilistic Model Checking

Authored by

Sobia Ashraf, Iram Tariq Bhatti, and Osman Hasan

Date: October 7, 2024

School of Electrical Engineering and Computer Science

National University of Sciences and Technology (NUST),

Islamabad, Pakistan

Abstract

Protection systems in power distribution networks (PDNs) are responsible for monitoring the electrical networks, detecting faults, and tripping the breaker to isolate the faulted section of the network. Ensuring reliability and safety in Multi-agent systems (MAS) based protection systems is vital for the smooth functioning of PDNs during emergency situations. Therefore, we propose to use probabilistic model checking, a formal verification technique, to provide a framework for the analysis of Multi-agent systems (MAS) based protection systems. In this regard, we have developed formal Markovian models of protection system components that can be used to model, analyze, and verify MAS-based protection systems. To illustrate the usefulness of the developed models, we have used them to verify and compare the reliability and safety of an auxiliary algorithm with the conventional protection algorithm using the PRISM model checker. The results show that the auxiliary algorithm is more reliable and safer than the traditional algorithm. The formal models of this study are available on our GitHub page [1].

KEY WORDS: Multi-agent System, Formal Verification, Probabilistic Model Checking, PRISM Model Checker, Reliability, Safety, Protection Systems.

[1] `https://sobiaatnust.github.io/Quantitative-Analysis-of-MAS-Based-Protection-Systems/`

Contents

Chapter 1

Introduction

A fault in an electrical power system is an abnormal condition that can arise due to internal or external factors, like equipment failures, human errors, abrupt changes in weather conditions such as lightning strikes, storms, heavy rains, or winds, which may interrupt the normal flow of power in the system. For example, a fault due to a short circuit can cause an excessive current flow in the network, which can damage/burn the equipment completely if exposed for a long duration, can cause electrical fires, or in the worst case, can take human/animal lives. The primary purpose of introducing protection in power distribution networks (PDNs) is to identify the location of the fault and isolate the faulty section from the rest of the healthy network for it to work normally. Relays and circuit breakers are deployed in PDNs for protection purposes, where the relay's job is to sense the fault current and issue a trip signal to the circuit breaker, which then automatically opens its contacts to immediately disconnect the short circuit path from the healthy network.

Integration of distributed generation (DG) units in PDNs affects the current flow in the network and imposes numerous challenges to the protection systems. Some of which include miscommunication among protection components, mal-operation of protection relays, the inability to detect the faults due to the varying fault current levels, and bidirectional power flow. Similarly, the magnitude and direction of the current flow in the network is also influenced by the penetration level, and the location of DGs in the system [7, 17, 20, 21, 24]. To ensure proper coordination and correct operation of the relays, it is necessary to update the relay settings according to the changes in the network. For this purpose, various multi-agent system (MAS) based protection schemes have been proposed to protect the DG-integrated PDNs [14, 22]. MAS are computational systems that can be used to represent complex systems with several inter-

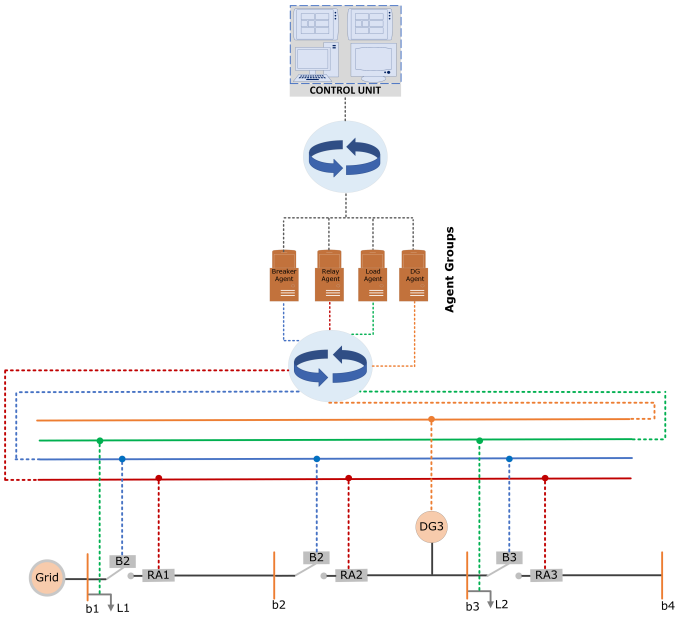

Figure 1.1: A typical MAS structure for PDN.

acting components where agents coordinate their efforts to achieve common goals such as task completion, problem resolution, or system optimization [16]. Fig. 1.1, shows a typical MAS deployment in a PDN environment. Relays, circuit breakers (CBs), loads, and DG agents make up the three-layer MAS architecture. According to the MAS definition, when a change occurs within a network, a disturbance is identified, and agents gather appropriate data. In the higher layer of the MAS, agent groups receive information from the agents and transmit it to the central controller, which acts as the topmost layer responsible for organizing the lower-level agents to facilitate effective collaboration [14]. However, with increasing deployment of DGs into the grid, these methods suffer from various drawbacks, such as a high dependency on the central controller, as its failure may lead to protection mal-operation. Moreover, if a fault occurs during the relay settings update process, this may result in miscoordination among relays. To avoid wrong operations, an additional relay is required to be used in case of emergency. Thus, an auxiliary algorithm is proposed in [8] to substitute MAS-based schemes during emergency conditions. This approach utilizes the protection and signals dispatching features of modern relays along with supervisory service to ensure fault clearance in an efficient and timely manner [8].

Traditionally, the reliability of protection systems in PDNs is analyzed using numerical and simulation-based techniques [2, 4, 19]. The numerical techniques involve computer arithmetic, rounding-off errors, and avoidance of real-time possible/unforeseen situations, thus leading to inaccurate and incomplete analysis. Similarly, in the simulation-based analysis due to high computational requirements for exhaustive simulations, the reliability aspects are usually assessed

through a sampling-based approach, and thus all the possible scenarios are not considered. Therefore, these analysis techniques cannot ascertain a robust and error-free system that can lead to disastrous consequences on the operations of power grids due to their safety-critical nature. For instance, the famous blackout in the United States and Canada in 2003 affected almost 55 million people [6] and was a result of an inaccuracy in the system analysis. So, a rigorous and accurate analysis is required to evaluate the reliability and safety of the protection algorithms in PDNs.

To overcome the above-mentioned limitations associated with the traditional analysis techniques, probabilistic model checking has been used for evaluating the reliability of protection systems in PDNs [1, 12, 15, 18, 23]. Model checking [5] is a formal verification approach in which the system behavior, expressed as a state transition system, and its desired properties, expressed in temporal logic, are fed to an automatic verification tool. The tool exhaustively traverses the entire state-space of the system and ascertains if the given system behavior exhibits the desired properties or not. Probabilistic model checking [5, 9] is a variant of model checking that allows for the verification of probabilistic temporal properties for Markovian models. It has already been used to estimate the probability of transmission network failure by utilizing the data measured by phasor measurement units (PMUs) as a backup protection system [18]. Moreover, the integrated model of fault detection, isolation, and recovery (FDIR) with power line carrier (PLC) and wireless communication networks has also been verified using the probabilistic model checker PRISM [23]. Similarly, the reliability analysis of the relay-protected component has also been conducted using model checking in [1, 12, 15]. The formal models of conventional and dual-setting directional overcurrent relays, in particular, have been utilized to evaluate the performance of a three-bus network in [1, 3]. However, this model lacks the signal dispatching and auxiliary functionalities of digital relays, with no DGs and circuit breaker models. Therefore, we propose to build the formal model of a digital relay equipped with the functionality of signal dispatching and auxiliary services, which can be utilized for analyzing MAS-based protection systems along with the formal models of DGs and circuit breakers. Furthermore, to illustrate the effectiveness of this model, we formally analyze the reliability of a common MAS-based scheme during emergency fault conditions using an auxiliary fault-clearing algorithm proposed by Fani et al. [8]. This type of analysis is vital in evaluating the reliability and safety of the power system to ensure faster fault clearing, fewer undesirable operations, and an uninterrupted power supply.

1.1 Our Novel Contribution

Our main contribution in this work is to develop a generic formal probabilistic model of a digital relay with protection, signal dispatching, and supervisory service capabilities. Using this relay model and models of other supporting components, we have built a formal model of an auxiliary fault-clearing algorithm supporting MAS-based schemes and verified its reliability and safety operations with the help of the following properties:

- Likelihood of successful isolation of faulty section (Reliability)
- Chances of the system going into a complete failure state (Reliability)
- Probability of false tripping (Safety)
- Possibility of the system entering the danger zone (Safety)

These properties describe the ability of the protection algorithm to ensure the safe and reliable operation of the power system and to avoid harm or damage to people, property, or the environment. The performance and behavior of these properties must be carefully analyzed and evaluated to ensure the overall safety and reliability of the protection system. Using these properties, a comparative analysis of a common MAS-based scheme with the auxiliary algorithm is also given using our formal models.

The rest of the report is structured as follows. Chapter 2 provides a brief overview of probabilistic model checking, protection systems in PDN, and digital relay structure to facilitate the understanding of the rest of the report. Chapter 3 describes the proposed methodology. Chapter 4 deals with the formal modeling of different PDN components. Moreover, in Chapter 5 the formalization of relay agent-based fault clearing algorithms is presented. Chapter 6 presents a detailed formal analysis of a PDN using the formal models. Finally, Chapter 7 provides the conclusion.

Chapter 2

Background

2.1 Probabilistic Model Checking and PRISM

Model-checking is a model-based automatic formal verification technique, used for the verification of reactive systems [5]. Probabilistic model checking is used for the verification of systems that exhibit randomness. PRISM [13], a probabilistic model checker supports probabilistic verification and can provide useful quantitative insights regarding the performance of protection algorithms. It offers a GUI with an additional simulator tab for behavioral testing. PRISM can sometimes suffer from state space explosion problems due to the large state space of complex networks. However, this issue can be resolved by developing more abstract and property-specific models. PRISM supports different model types that can be used to represent and analyze systems with probabilistic behavior. Some of the commonly used model types in this regard are discrete-time Markov chains (DTMCs), continuous-time Markov chains (CTMCs), Markov decision processes (MDPs), and stochastic game models. The models are specified using a state-based PRISM language. The property specification languages available in the PRISM are linear temporal logic (LTL), computational tree logic (CTL), and probabilistic computational tree logic (PCTL) [5]. PRISM gives the verification results as true or false for the LTL and CTL properties and an estimate of the probability in the case of PCTL properties. Guarded commands are used to develop the Markovian model of a given system. The syntax for the PRISM commands is as follows:

```
[action] guard -> <prob_1> : <update_1> + . . . + <prob_n> : <update_n> ;
```

A guard is a predicate over all the system variables, and a transition can only occur if the guard condition holds true according to the pre-defined state transition probabilities. Moreover, the

guarded commands can be optionally combined with action labels to synchronize two or more state transitions. The symbol "$->$" denotes the transition. Each $< prob\_i >$ represents a probability value associated with the transition, and $< update\_i >$ represents the updated state of variables that occur when this transition is taken. A single guard can have multiple update assignments separated by the "+" symbol such that the sum of all $< prob\_i >$ must be equal to 1. However, at a given time only one $< prob\_i > < update\_i >$ can occur. There can be multiple probabilistic choices, each with its probability and update assignment. The plus symbol "+" is used to separate multiple probabilistic choices. The total sum of probabilities associated with all possible outgoing transitions from a given state must be equal to 1. PRISM also allows module renaming, which facilitates more expressive and adaptable modeling, especially for systems with recurring or similar modules/components. The module name, variables, action labels, and constants are replaced with new and unique names. Additionally, identifiers including action labels, constants, and functions can be modified in a similar manner.

2.2 Protection Systems in PDNs

PDNs utilize protective components to quickly detect and locate faults, isolating the faulty section from the rest of the network. When it comes to short-circuit faults, the protection components should be sensitive enough to operate at minimum fault currents without triggering during routine events like load changes [11]. Fig. 2.1a shows a single-line representation of a radial PDN. The PDN has three distinct protection zones, labeled as Zone Z1, Z2, and Z3. Each zone is protected by a set of over-current relays and circuit breakers, labeled as RA1, RA2, and RA3, and B1, B2, and B3, respectively. Relay RA3 protects Zone Z3, while Relay RA2 is the primary relay of Zone Z2 and provides backup to Relay RA3. In case the relay RA3 or its associated circuit breaker B3 fails to operate, relay RA2 operates and sends a signal to its breaker B2 to isolate both zones Z2 and Z3 while maintaining a proper coordination time margin (CTM) with RA3. Likewise, relay RA1 provides primary protection to Zone Z1 and backup protection to zones Z2 and Z3, respectively.

For the overcurrent relays, Equation (2.1) [22], is used to determine the CTM between the primary and backup relays.

$$\frac{TDS_p \times a_p}{c_p^{n_p} - 1} - \frac{TDS_b \times a_b}{c_b^{n_b} - 1} \geq CTM \tag{2.1}$$

Where subscripts p, and b, represents the primary and backup relays, a, and n are the relay

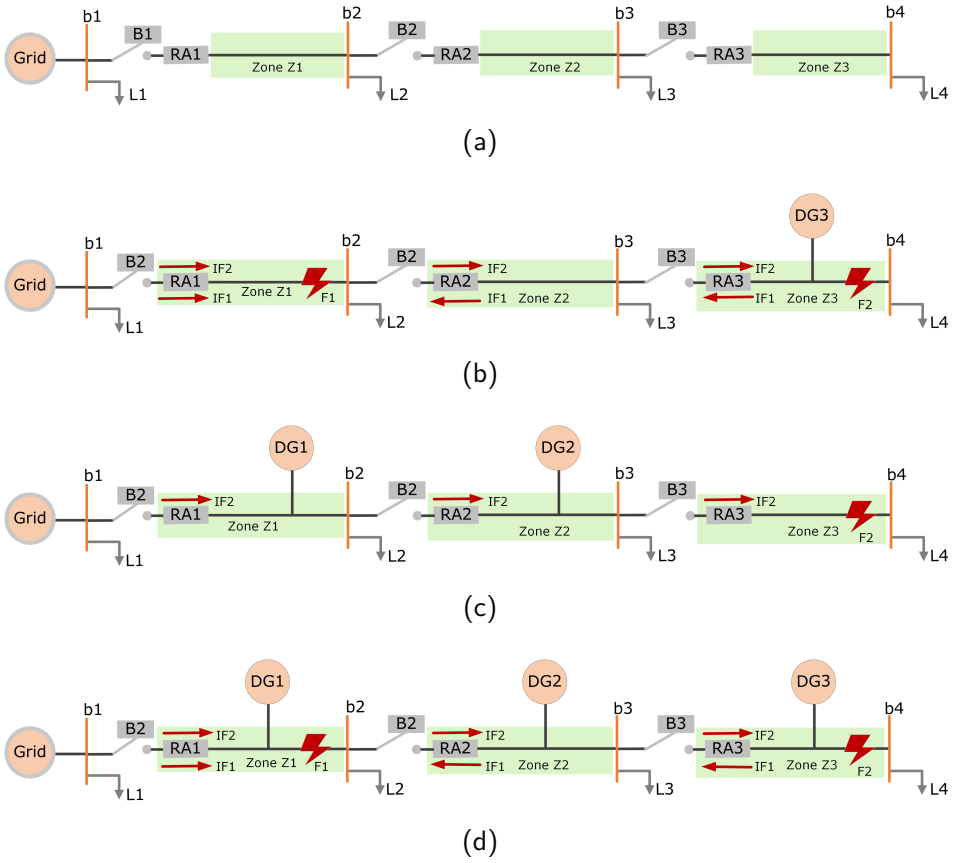

Figure 2.1: A Single Line Diagram of a PDN (a) No DG Unit (b) One DG Unit (c) Two DG Units (d) Three DG Units

characteristic constants, and TDS represents the time dial settings of the relay. The fault to pick up current ratio is given by c. The CTM ensures the coordination between primary and backup relays. The desired CTM margin is between 300 to 400 ms as stated in [10].

According to Equation (2.1), c can be changed by changing the fault current levels. The fault current level can be varied by varying the capacity and location of DGs which can increase/decrease the relays' operating time. For example, based on the location and size of DGs in a network, the following three possible coordination scenarios can occur from the protection perspective:

- 0.3(s)<=CTM<=0.4(s): In this case, the coordination margin is within the allowable range; therefore, primary and backup relays operate according to their pre-defined settings, and there are no chances of system maloperation.
- CTM<0.3(s): In this case, the operating times of both primary and backup relays become very close to each other. Therefore, it may lead to false tripping of the backup relay (i.e., the backup relay might trip unnecessarily in addition to the primary relay).

- CTM>0.4(s): In this scenario, when the primary relay fails to respond to a fault, the backup relay operates after a large time delay, leaving the system exposed to the fault for a long period of time. In such a condition, the line conductors may reach their thermal limits, putting the system at risk.

To understand the influence of DGs on the protection coordination of relays, consider if only DG3 is present in the PDN and a Fault F2 occurs in Zone Z3, as depicted in Fig. 2.1b. The fault current IF2 through Relays RA2 and RA3 is identical to the one that is injected from the main grid. Relay RA3 is the primary relay and Relay RA2 provides backup in a coordinated manner. However, if Fault F1 occurs in Zone Z1, upstream of both Relays RA2 and RA3, then the fault current IF1 of RA2 and RA3 is equal to the current contribution from DG3. Moreover, the fault current IF1 through Relay RA1 is equal to the one that is injected from the main grid. Relay RA2 is the primary relay, and Relay RA3 is the secondary relay under these circumstances. If DG1 and DG2 are installed into the PDN as shown in Fig. 2.1c, and Fault F2 occurs in Zone Z3, the Relays RA2, and RA3 experience higher fault current values due to the fault current contribution of the DGs. In this scenario, the relay settings should be updated according to the new values of minimum and maximum fault current. Next, assume that a Fault F2 occurs and the three DGs DG1, DG2, and DG3 are incorporated into the PDN as shown in Fig. 2.1d, and thus the fault current increases significantly. In this scenario, Relays RA2 and RA3 may operate simultaneously, or RA2 may operate before RA3, resulting in protection miscoordination between RA2 and RA3. Similarly, if a Fault F1 occurs inside Zone Z1, as depicted in Fig. 2.1d, the fault current IF1 through Relay RA2 is the sum of DG2 and DG3 fault currents, while the fault current IF1 seen by RA3 is the DG3 fault current. In this condition, if Relay RA2 fails to provide primary protection, the backup Relay RA3 may not operate within CTM due to its large operating time, thus resulting in protection miscoordination between RA2 and RA3.

2.3 Digital Relay Structure

Digital relays are intelligent electronic devices (IEDs), which are equipped with numerous functionalities like protection, watchdog, supervisory, control, metering, data accessing and sharing, and communication, just to name a few. A typical structure of a digital relay, as shown in Fig. 2.2, represents two main relay functions, i.e., the communication and other relay functionalities. The communication section is further divided into two subsections: data sharing/assessing and signal dispatching. The data sharing section is responsible for sharing or

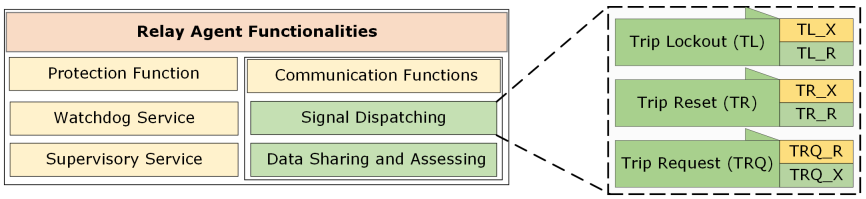

Figure 2.2: Digital Relay Structure

assessing the data between relays and different communication layers, while signal dispatching is used to transmit and receive signals between neighboring relays [8].

A brief description of the three binary signals and the auxiliary services including the watchdog and supervisory service is given below:

- Trip Lockout (TL_X, TL_R): When a fault occurs, the relay closest to the fault picks up and sends the TL_X signal to the nearby relays in order to prevent the unnecessary tripping of the backup relays. The letter X with the TL represents the outgoing signal, whereas R represents the incoming trip lockout signal.

- Trip Reset (TR_X, TR_R): When the main relay operates, it issues a TR_X command to its backup relay to release it from the locked state. Therefore, a relay with TL_R command remains in the locked state unless it receives a TR_R reset command.

- Trip Request (TRQ_X, TRQ_R): When a relay receives a trip request TRQ_R command from its neighboring relay, it operates instantly without any coordination delay.

- Watchdog Service: Watchdog service continuously monitors the health of the relay. If an error, fault, or failure occurs in the relay, it disables all the protection functions. In order to prevent the mal-operation of the relay.

- Supervisory Service: Supervisory service is the supreme head of the digital relay and continuously monitors the relay status and signal dispatching services. If the main relay fails to trip and, at the same time, an issue occurs in transmitting or receiving the signals due to communication failure, then the backup relays are unable to operate, thus making it impossible to release the backup relays from the lockout state. To avoid this issue, the supervisory service is activated after a predefined time and cancels out all the previous commands in the backup relay, including the trip lockout command, and also sends a command to open the circuit breaker.

Chapter 3

Methodology

PRISM supports probabilistic verification and can provide useful quantitative insights regarding the performance of protection algorithms. It offers a GUI with an additional simulator tab for behavioral testing. A major drawback of PRISM is that it usually suffers state space explosion problems due to the large state space of complex networks. However, this issue can be resolved by using more abstract and property-specific models. To develop the formal model of the protection system of PDNs we propose to use the discrete-time Markov chains (DTMCs) [13]. DTMCs allow us to capture the probabilistic behavior of the system. The formal models of the individual components of PDN, i.e., the digital relay equipped with communication and protection functions, the DG, and the circuit breakers can be used to model and verify any arbitrary MAS-based system. The proposed methodology is depicted in Fig. **??**. In the first step, the formal models of the individual components of PDN, i.e., protection relays, DGs, and circuit breakers, are developed. In the next step, the formalization of conventional and auxiliary protection algorithms is performed. Furthermore, a complete protection system model of PDN is developed by integrating the protection algorithms into the individual models. Once the complete formal model is developed, its functional correctness is checked using the PRISM simulator. This allows debugging the model for any functional errors and undesired scenarios through random path selection prior to the verification. Once the model is functionally accurate, probabilistic verification is performed to determine the reliability and safety properties of the system. In this regard, we have proposed to determine the likelihood of successful isolation of faulty section, the possibility of isolation failure, chances of false tripping (i.e., the backup relay operates when it is not desired to operate), and the possibility of the system to undergo a risk (i.e., system remain exposed to the fault for a very long time). These properties can be

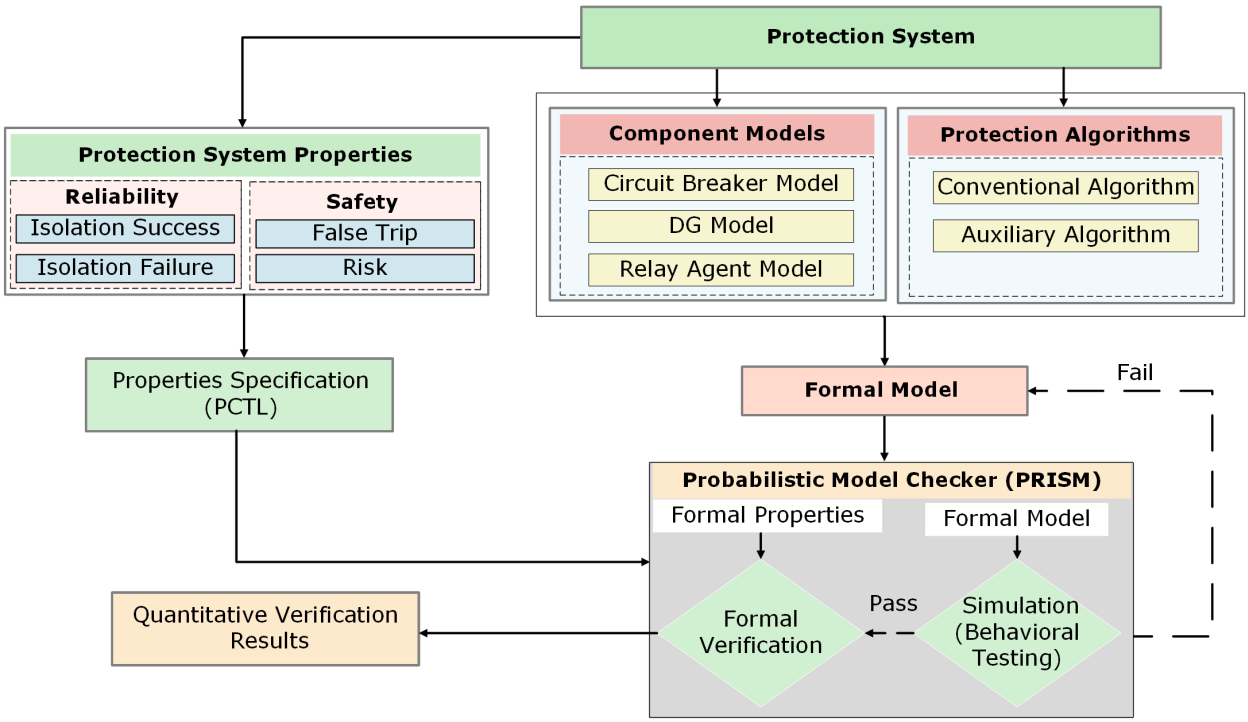

Figure 3.1: Proposed Methodology

expressed in PRISM as follows:

1. `P=?[F "Isolation Success"]`
2. `P=?[F "Isolation Failure"]`
3. `P=?[F "False Trip"]`
4. `P=?[F "Risk"]`

The formal model of the protection system and its desired reliability and safety properties, specified in PCTL, are then fed to the probabilistic model checker PRISM, which automatically traverses the entire state-space of the model and gives the quantitative verification results.

Chapter 4

Formal Modeling of Protection System Components

4.1 Circuit Breaker and DG Model

Circuit breakers are used in PDNs to isolate the faulty network from the rest of the healthy network in case of short circuits or other faults. Whenever a fault occurs in PDN, the relay connected to the circuit breaker detects the fault and sends a trip signal to the circuit breaker, which prompts the breaker to open its contacts. The initial status of the circuit breakers determines the configuration of a PDN. Initially, a circuit breaker can be either open or closed. If it is closed and the breaker command (*BC=1*) sent by the respective relay as shown in Listing 1, is high in the presence of a fault, it either opens or fails to open.

The DGs connection and disconnection give information about the current injected into the system. For the sake of simplicity and considering the objective of our analysis, we have abstracted the behavior of DGs as a constant current source. As shown in Listing 1, whenever a DG is present in the network (*DG=2*), it injects a constant non-zero current (*IDG=1*) into the network. Moreover, the DGs and breakers status is accessible to all the relay models.

4.2 Relay Agent Model

A digital relay block diagram is depicted in Figure 4.1. The relay has a built-in protection mechanism that activates its operation in the event of a fault in its zone or a neighboring zone. In addition, it encompasses the relay's watchdog, supervisory, and signal dispatching services.

```
                    ////  Circuit Breaker Module  ////

module Breaker

B:[0..3];
// 0: Initial state  // 1: Open
// 2: Close  // 3: Fail to open
// BRK: Probability of breaker failure
// BC: Breaker command   // isol: Isolation success

[] B=0 & BC=0 -> 0.5:(B=1) + 0.5:(B=2);

[] B=2 & BC=1 -> 1-BRK:(B=1) & (isol=true)  + BRK:(B=3) & (isol=false);

endmodule

                        ////  DG Module  ////

module DG

IDG:[0..1];
// IDG: DG's current contribution
DG:[0..2];
// 1: DG not connected  // 2: DG connected

[] DG=0 & IDG=0 ->  0.5:(DG=1) & (IDG=0) + 0.5:(DG=2) & (IDG=1);

endmodule
```

Listing 1: Circuit Breaker and DG Module

The watchdog service monitors the relay' s physical health and detects internal errors. The supervisory service oversees the relay's operation and trips the breaker in case of relay failure, and the signal dispatching sends lockout, reset, and request signals as needed. Depending on the level of details required for the verification purpose, a formal model of the digital relay is created to capture its essential behaviors accurately with some abstractions to avoid state-space explosion in the verification phase. For simplification and to align with the objective of our analysis, the relay's timing and measurement functions are not included in this model. Following a "Fault", the relay `Protection` module, as given in Listing 2, determines the relay modes, i.e., whether it is in `Active` mode, `Passive` mode, `Lockout` mode, `Reset` mode, `Trip` mode, or `Fail` mode depending on the following conditions:

- In the initial state when the relay senses a non-zero fault current, it transitions to `Active` ($RA\_p{=}5$) mode. Conversely, if the fault current is zero it switches to `Passive` ($RA\_p{=}6$) mode.

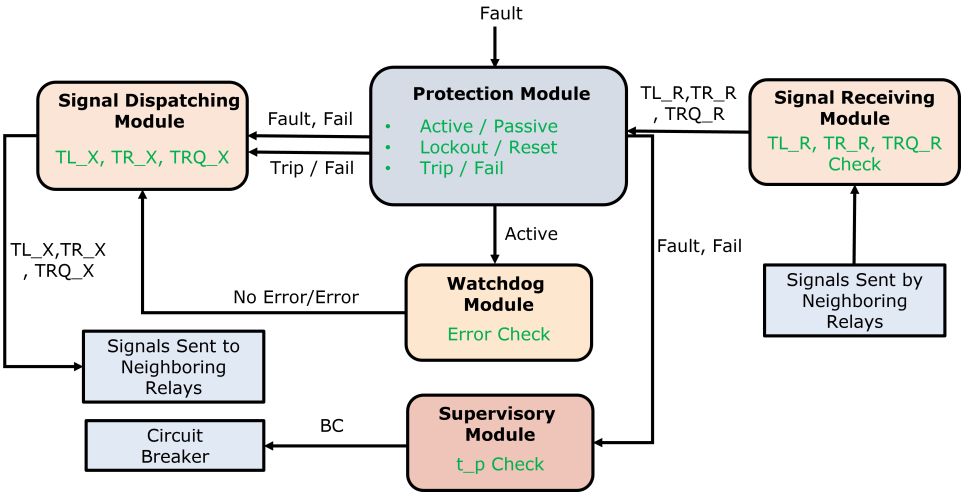

Figure 4.1: Relay Block Diagram with Auxiliary Functions

- The `Watchdog` module, checks the relay for internal error as shown in Listing 2. If there is "No Error" ($WD\_p=2$) in the relay, then the relay operates and goes to either the `Trip` ($RA\_p=1$) mode or `Fail` ($RA\_p=2$) mode. Conversely, when there is an active "Trip Lockout" command the relay switches to `Lockout` ($RA\_p=3$) mode.

- The relay remains in the `Lockout` mode until it receives a "Trip Reset" command ($TR\_Rp=1$) from its b^{th} neighboring relay. Upon receiving the "Trip Reset" command, it moves to the `Reset` ($RA\_p=4$) mode.

- When the relay is in the `Reset` mode or `Active` mode, and it receives a "Trip Request" command ($TRQ\_Rp=1$) from its neighboring relay, then it transitions to either `Trip` ($RA\_p=1$) mode or `Fail` ($RA\_p=2$) mode.

- Whenever the relay is in `Trip` mode, then it issues a breaker command ($BC\_p=1$) to its respective breaker.

The `Signal Dispatching` module, as given in Listing 2, issues the "Trip Lockout" signal (TL_X), "Trip Reset" signal (TR_X), and the "Trip Request" (TRQ_X) signal according to the operation status of the relay. During the operation of relay the `Signal Dispatching` module issues a "Trip Lockout" command ($s\_p=1$) simultaneously. After the operation of relay, the `Signal Dispatching` module issues a "Trip Reset" command ($s\_p=2$) to reset the neighboring relays from lockout. Additionally, if the relay is in the `Fail` mode or there is an "Error" in the relay, or if the relay is in the `Trip` mode but the breaker fails to operate upon receiving the breaker command from the relay, then the `Signal Dispatching` module issues a "Trip Request" ($s\_p=3$) command.

```
                    ////    Protection Module  ////

module Protection
RA_p:[0..6];
// 0: Initial state  // 1: Trip   // 2: Fail
// 3: Lockout       // 4:Reset   // 5: Active
// 6: Passive      // RA_p: Primary relay  // RA_b: Backup relay
BC_p:[0..2];
// 1: Breaker signal sent           // 2: Signal not sent
// IED: Relay Failure Probability  // IRp_F: Relay fault current

[] RA_p=0 & Fault=true & IRp_F=0  ->  (RA_p=6);

[] RA_p=0 & Fault=true & IRp_F>0  ->  (RA_p=5);

[lock] RA_p=5 & WD_p=2 & (TL_Rp=0|TL_Rp=2) -> 1-IED:(RA_p=1) + IED:(RA_p=2);

[] RA_p=5 & WD_p=2 & TL_Rp=1  ->  (RA_p=3);

[] RA_p=3 & TR_Rp=1  ->  (RA_p=4);

[] (RA_p=4|RA_p=5) & TRQ_Rp=1 -> 1-IED:(RA_p=1) + IED(RA_p=2);

[] RA_p=1 & BC_p=0 -> 1-COM:(BC_p=1) + COM:(BC_p=2);

[] sv_p=1 & (BC_p=0|BC_p=2) -> (BC_p=1); ^^I

endmodule

                    ////    Watchdog Service   ////
module Watchdog
WD_p:[0..2];
// 0: Initial state      // 1: Relay has error
// 2: Relay has no error // err: Probability of error

[] WD_p=0 & RA_p=5 -> err:(WD_p=1) + 1-err:(WD_p=2);

endmodule

                    ////  Signal Dispatching   ////

module Signal Dispatching
s_p:[0..5];
// 0: Initial state   // 1: TL_X sent
// 2: TR_X sent       // 3: TRQ_X sent
// 4: TRQ_X not sent  // 5: TL_X not sent
// COM: Probability of communication failure
// CTM: Coordination margin    // 1: Normal   // 2/3: Out of Range

[lock] s_p=0 & (WD_p=2) ->  1-COM:(s_p=1) + COM:(s_p=5);

[opr] RA_b=3 -> (s_p=2);

[] s_p=0 & WD_p=1 -> 1-COM:(s_p=3) + COM:(s_p=4);

[] s_p=2 & (RA_p=2|BC_p=2|(BC_p=1 & B_p=3)) -> 1-COM:(s_p=3) + COM:(s_p=4);

endmodule
```

Listing 2: Different Relay Modules

The `Supervisory` module, as described in Listing 3, activates when both the primary and backup relays or associated breakers fail to clear the "Fault", and the "Fault" persists for a long time, then after the (t_p=true) time has elapsed the `Supervisory` service is activated ($sv\_p=1$), and it sends a signal to the breaker. As we did not incorporate the timing in our model, therefore, in the `Supervisory` module, we have assigned equal distribution to the time elapsed. Additionally, the `Signal Receiving` module, as shown in Listing 3, caters to the possibility that the signals sent by one relay are not received by the neighboring relay due to a communication failure. Throughout the text, the primary and neighboring/backup relays are represented alternatively using the subscripts "p" and "b".

```
                    ////  Signal Receiving   ////

module Signal Receiving

TL_Rp:[0..2];     // Trip lockout received
TRQ_Rp:[0..2];    // Trip request received
// 0: Initial state    // 1: Signal received
// 2: Signal not received
// s_b signal sent by the neighboring relay

[] TL_Rp=0 & s_b=1  -> 1-COM:(TL_Rp=1) + COM:(TL_Rp=2);

[] TRQ_Rp=0 & s_b=3 -> 1-COM:(TRQ_Rp=1) + COM:(TRQ_Rp=2);

endmodule

                    ////  Supervisory Service   ////

module Supervisory

sv_p:[0..1];   // 0: Initial state
// 1: Supervisory service activated
t_p: bool init false;     // t_p: time elapsed

[] (t_p=false) & (TRQ_Rp=2|TL_p=1|((RA_p=2) & (B_b=2|B_b=3)))
   &((CTM=2|CTM=3)|WD_b=1) ->  0.5:(t_p=false) + 0.5:(t_p=true);

[] (t_p=false & BC_p=2) & (B_b=2|B_b=3) & ((CTM=2|CTM=3)|WD_b=1)
    ->  0.5:(t_p=false) + 0.5:(t_p=true);

[] sv_p=0 & t_p=true  -> (sv_p=1);

endmodule
```

Listing 3: Different Relay Modules

Chapter 5

Formalization of Relay Agent Based Fault Clearing Algorithms

5.1 Conventional and Auxiliary Protection Algorithms

Fig. 5.1, shows the flow chart of the relay agent-based conventional protection algorithm. Upon the occurrence of a fault, the initial network configuration and breaker statuses are identified. The primary (PR) and backup relays (BR) exchange information regarding fault current and operation status. The PR watchdog service checks the relay for internal errors, and if the relay is healthy, the CTM between PR and BR is calculated using Equation 2.1. DGs can have a negligible impact on relay coordination if they are placed upstream, away from the fault point and relays. Otherwise, if they are located between the primary and backup relays close to the fault point, then the coordination between the relays is disturbed. When the CTM is within the normal range, PR and BR operate normally to isolate the faulty section. However, if the CTM is less than 0.3, the PDN may experience false tripping when both PR and BR operate. If the CTM exceeds 0.4 and PR fails to operate, the BR may not be able to respond in a timely manner, putting the system at risk.

Typical MAS-based schemes with central control use wide-area communication to detect the network configuration/scenario changes and determine the new settings for the respective relays [14]. For a successful fault clearance, the suitable relay settings should be updated by the upper control level. But, if a penetration variation event and a sudden fault occur at the same time, the current relay settings cannot clear the fault, thus resulting in mal-operation or delayed operation as shown in Fig. 5.1. To ensure proper coordination, appropriate group settings need

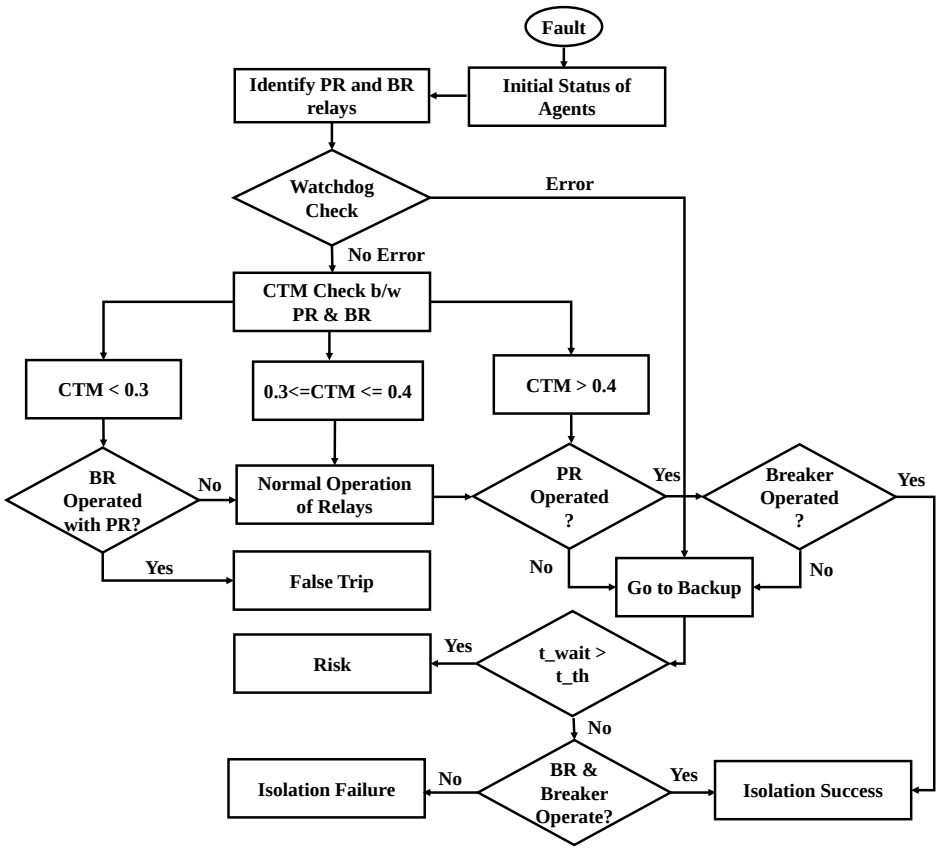

Figure 5.1: Flowchart of Conventional Protection Algorithm

to be updated in the relays after every penetration variation. However, in a situation where a fault occurs while the relay settings are being updated due to time lag or communication failure, the relay coordination may be disrupted and there is no guarantee of having a valid relay operation.

To cope with this problem, an auxiliary protection algorithm is proposed in [8]. The flowchart depicted in Fig. 5.2, demonstrates how this algorithm can be used to clear the fault in an emergency scenario. Once a fault occurs, the network identifies PR and BR agents, followed by the Watchdog service of PR to perform check for internal errors. If an error is present, then the PR sends a "Trip Request" to its BR, and upon receiving the request, the BR operates instantly. However, if PR encounters an internal error, it may not be able to send the "Trip Request" signal. In this case, if the BR is not in lockout state due to the "Trip Lockout" signal, it operates normally and clears the fault. Otherwise, the BR activates its Supervisory service after a predefined time (t_b) to trip the circuit breaker and clear the fault. On the other hand, when the PR Watchdog service indicates no internal error, and the CTM between PR and BR lies within an acceptable range (i.e., 0.3<= CTM<=0.4), both relays proceed with their normal operation. In case of violation of CTM from the normal range, the following procedure, as shown

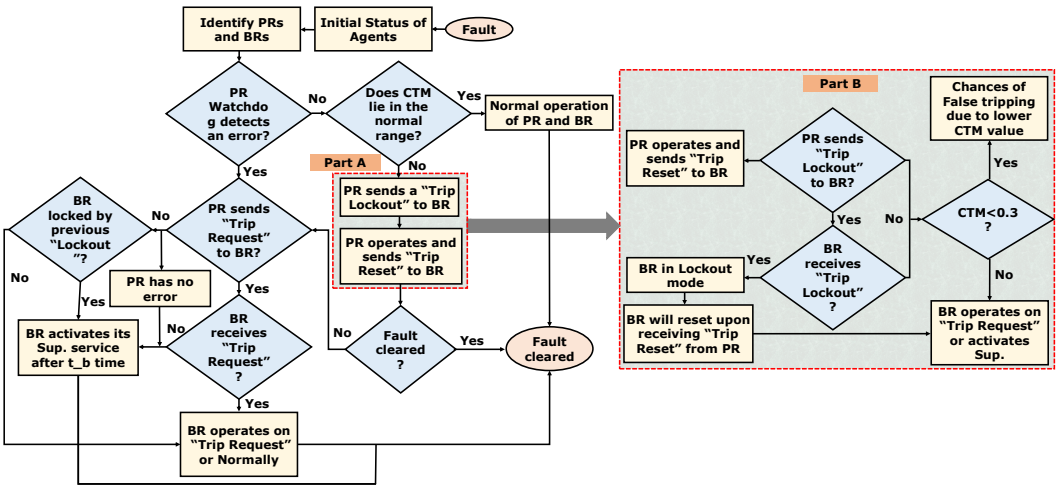

Figure 5.2: Flowchart of Auxiliary Algorithm

in Fig. 5.2, Part A is followed.

- The PR initiates a "Trip Lockout" signal to the BR.
- The PR operates and simultaneously dispatches a "Trip Reset" command to the BR.
- In case the fault is not cleared, the PR sends a "Trip Request" to the BR to isolate the fault immediately.
- If the "Trip Request" signal is not sent by PR or the BR fails to receive this signal, the BR starts its Supervisory service after t_b time to isolate the fault from the rest of the network.

It is important to note that the Auxiliary algorithm [8] does not consider the impact of the failure of the "Trip Lockout" signal on the performance of BR. This limitation is overcome by incorporating Part B into the flow of the Auxiliary algorithm, as shown in Fig. 5.2. When the CTM is not in range, and the "Trip Lockout" signal is either not sent by PR or received by BR, thus, the operation of BR is not locked. In this case, if the value of CTM is less than 0.3, the BR may mal-operate and cause false tripping. But if CTM exceeds 0.4, then the BR either operates on receiving the "Trip Request" signal, or it activates the Supervisory service after t_b time elapses. In order to verify the effectiveness of our proposed framework, we have considered a practical PDN in the next section.

Interaction between Modules and Model Generation

In this subsection, we have covered the interaction between different modules in MAS-based scheme using the state-space representation, as shown in Fig. 5.3. Each double circle represents

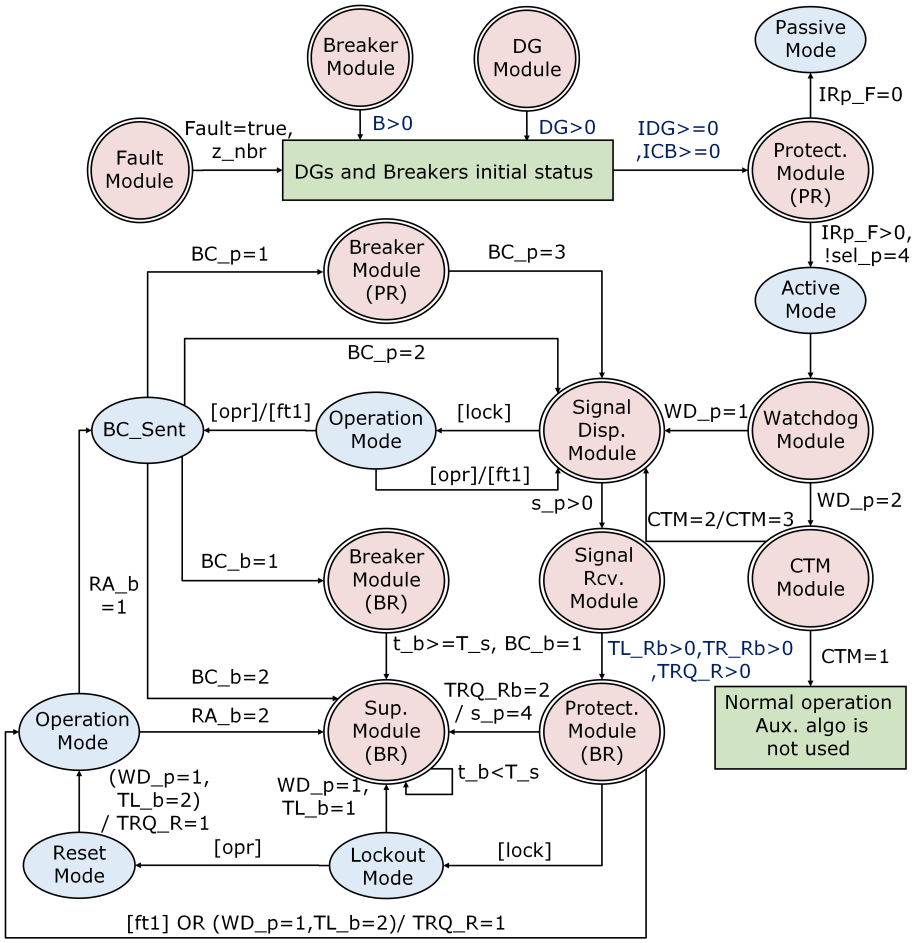

Figure 5.3: Interaction Between Different Modules

a PRISM module, and the oval shape is used to depict the local states associated with the protection module. The transition conditions and the action labels used for synchronism between different modules and local states are shown with black color, while the blue color is used to show information sharing among different modules during the interaction. Throughout the text, the primary and neighboring/backup relays are represented alternatively using the subscripts "p" and "b". In the first step, the status of all the breakers and DGs is checked in the network to determine the network configuration and the relay fault current. Whenever a fault occurs, the `Protection` module of each relay agent, as shown in Listing 4, determines the infected fault zone based on the selectivity parameter (*sel_p* (for primary relay) or *sel_b* (for backup relay)), computed by taking the difference of the fault zone number (*z_nbr*) and the relay number (*r_nbr*). If the value of *sel_p or sel_b* lies between 0 to 3, and the relay agent senses a non-zero fault current (i.e., *IRp_F>0 or IRb_F>0*), then it transitions to the `Active` mode. Otherwise, the relay agent does not participate in the protection process, and it remains in the `Passive` mode. When the value of *sel_p=0 or sel_b=0* with a non-zero fault current, it implies that the

fault has occurred in the same zone as of the relay agent, and it will act as a PR agent. Otherwise, it indicates that the fault exists in the neighboring zone and the relay acts as a BR agent. Let's assume that p^{th} relay is acting as PR and b^{th} relay is acting as BR here. After determining the `Active` mode, the PR `Watchdog` module checks for internal errors in the relay agent. If the PR agent is healthy (i.e., *WD_p=2*), then `CTM` is checked to ensure coordination between the PR and BR agents. Up to this point, the working of the traditional and the auxiliary algorithm is exactly the same. Next, the conventional algorithm operates according to Fig. 5.1. Whereas the auxiliary algorithm follows Fig. 5.2. It uses the `Signal Dispatching` module as discussed in Listing 2, to send the BR agents to the `Lockout, Reset`, and `Operation` mode according to the *CTM* values. During the *CTM* check, if the value of *CTM* is within the acceptable range (i.e., *CTM=1*), then there is no need for an auxiliary algorithm, and the relays proceed with the normal operation. In case the *CTM* range is violated (i.e., *CTM=2 or CTM=3*), the PR initiates a "Trip Lockout" command (*s_p=1*) to its BR agent and goes to the `Operation` mode. During the `Operation` mode, it sends a "Trip Reset" command (*s_p=2*) to release the BR from the `Lockout` state. Moreover, if the PR or its associated breaker fails to clear the fault, it will issue a "Trip Request" command (*s_p=3*) to the BR, requesting it to clear the fault instantly. Additionally, if the PR relay is faulty (i.e., *WD_p=1*), then it sends a "Trip Request" command (*s_p=3*) command to its respective BR to clear the fault. However, if, due to a communication failure or an internal error, the PR agent is unable to send the "Trip Request" signal (*s_p=4*), then the BR agent represents a non-deterministic behavior of being either in the `Lockout` mode, `Reset` mode or `Active` mode. In this case, if the BR agent is in the `Active` mode or `Reset` mode, it will transit to the `Operation` mode. Otherwise, the `Supervisory` module of BR will be activated after a predefined time interval (*T_s*) and cancel out all the previous commands in the BR, and send a signal to the breaker. Upon successful tripping, the relay agents send a command to the `Breaker` (*BC_p=1 or BC_b=1*) module. Moreover, if the PR agent or its breaker did not operate, and the BR agent is also stuck in the `Lockout` state, or it did not receive the "Trip Request" signal (*TRQ_Rb=2*), then, after a predefined period, the BR `Supervisory` module activates the breaker command (*BC_b=1*). Additionally, as shown in Part B of Fig. 5.2, if the CTM is less than 0.3s (i.e., *CTM=2*), and the communication between PR and BR agents is disrupted for any reason, and the PR fails to send "Trip Lockout" command (*s_p=5*) or the BR does not receive the lock signal (*TL_Rb=2*), then the BR goes to the `Operation` mode and may operate unnecessarily, leading to a false tripping scenario. More details about the formalization of these algorithms can be accessed from the source code [1].

```
module Auxiliary Protection

RA_p:[0..6];
// 0: Initial state  // 1: Trip  // 2: Fail
// 3: Lockout  // 4:Reset  // 5: Active
// 6: Passive
sel_p:[0..4] init 4;
BC_p:[0..2];
// 1: Breaker signal sent  // 2: Breaker signal not sent
TL_p:[0..2];
// 1: Previous lockout  // 2: Not in prev. lockout
// r_nbr: Relay number  // z_nbr: Zone number
// IED: Relay Failure Probability

[] RA_p=0 & sel_p=4 & Fault=true & r_nbr>=z_nbr & B_p>0 & B_b>0
  -> (IRp_F=sum_of_upstream_resources_current) & (sel_p=r_nbr-z_nbr);

[] RA_p=0 & sel_p=4 & Fault=true & r_nbr<z_nbr & B_p>0 & B_b>0
   -> (IRp_F=sum_of_upstream_resources_current) & (sel_p=-(r_nbr-z_nbr));

[] RA_p=0 & sel_p=4 & IRp_F=0 -> (RA_p=6);

[] RA_p=0 & !sel_p=4 & IRp_F>0 -> (RA_p=5);

// When RA_p is acting as the main relay
[opr] RA_p=5 & WD_p=2 & sel_p=0 -> 1-IED:(RA_p=1) + IED:(RA_p=2);

[ft1] RA_p=5 & WD_p=2 & sel_p=0 -> 1-IED:(RA_p=1) + IED:(RA_p=2);

// When RA_p is acting as a backup Relay
[lock2] RA_p=5 & !sel_p=0 & IRp_F>0 & s_b=1 & TL_Rp=1  -> (RA_p=3);

[] RA_p=5 & CTM=3 & (s_b=5|TL_Rp=2)  ->  (RA_p=3);

[ft2] RA_p=5 & CTM=2 & (s_b=5|TL_Rp=2) ->  1-IED:(RA_p=1) + IED:(RA_p=2);
      ^^I
[opr2] RA_p=3 & s_b=2 -> (RA_p=4); //Reset

[] (RA_p=5|RA_p=4) & s_b=3 & TRQ_Rp=1 -> 1-IED:(RA_p=1) + IED:(RA_p=2);

[] RA_p=5 & s_b=4 -> 0.1:(RA_p=3) & (TL_p=1)+0.45:
   (RA_p=5)& (TL_p=2) + 0.45:(RA_p=4) & (TL_p=2);

[] RA_p=1 & BC_p=0  ->  1-COM:(BC_p=1) + COM:(BC_p=2);

[] sv_p=1 & (BC_p=0|BC_p=2) -> (BC_p=1);

endmodule
```

Listing 4: Auxiliary Algorithm Protection Module

Chapter 6

Formal Analysis of Protection Systems

6.1 Test System Description

A single-line diagram of PDN [8] depicted in Fig. 6.1, which is a part of a real network in Esfahan Iran, is taken as a case study for assessing the performance of our formal model. The network is grouped in four zones (Z1-Z4), having two feeders connected via SW breaker, and four relay agents (RA1-RA4) with their associated circuit breakers (B1-B4). The system also contains four DGs (DG1-DG4), which are installed on four buses b2, b3, b8, and b10. The system works under certain constraints that are applied to the initial status of breakers B1, B3, and SW, as mentioned below:

- If the SW breaker is closed, then either breaker B1 or B3 should be open
- If both the breakers B1 and B3 are closed then SW breaker should be open
- Both the breakers B2 and B4 can be either opened or closed

The above limitations lead to numerous possible switching configuration scenarios. Some of them are listed in Table 6.1. It is important to mention that the desired scenarios are those in which, following a fault, the PR and BR agents function to protect the system. In scenario SC 13, whenever a fault occurs in zone Z3 and breakers B1, B2, and B4 are open, then only relay RA3 participates in the protection process, and no other BR is available to check for the coordination criteria, hence, this is declared as an undesired scenario. Only scenarios SC 1, SC 3, and SC 6 are covered in the simulation-based paper [8], whereas our analysis covers all the possible

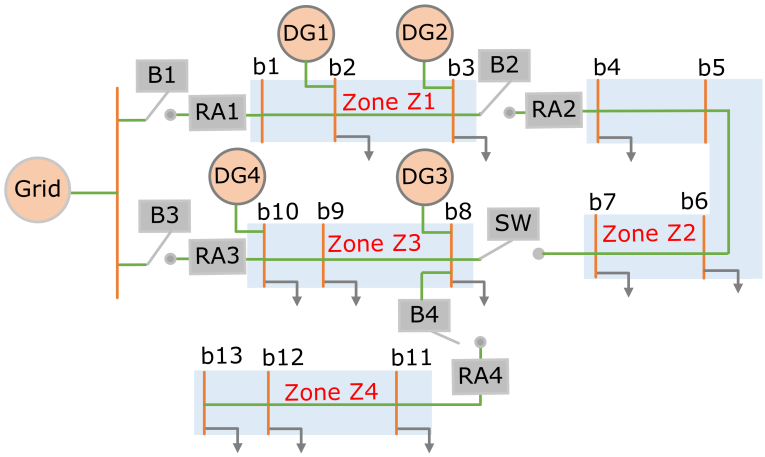

Figure 6.1: Single Line Diagram of Test System

Table 6.1: Some Possible Network Configurations

No.	Breakers Status	Possible Fault Zones	Participating Relays
SC 1	B1 open	Z1, Z2, Z3, Z4	RA2, RA3, RA4
SC 2	B1, B2 open	Z4	RA3, RA4
SC 3	B3 open	Z1, Z2, Z3, Z4	RA1, RA2, RA4
SC 4	B1, B4 open	Z1, Z2, Z3	RA2, RA3
SC 5	B3, B4 open	Z1, Z2, Z3	RA1, RA2
SC 6	SW open	Z2, Z4	RA1, RA2, RA3, RA4
SC 7	SW, B1 open	Z4	RA3, RA4
SC 8	SW, B2 open	Z4	RA3, RA4
SC 9	SW, B1, B2 open	Z4	RA3, RA4
SC 10	SW, B3 open	Z2	RA1, RA2
SC 11	SW, B4 open	Z2	RA1, RA2
SC 12	SW, B3, B4 open	Z2	RA1, RA2
SC 13	B1, B2, B4 open	Z3 (Undesired)	RA3 only

network scenarios (either desired or undesired) which can occur from the protection perspective by considering the impact of DGs connection/disconnection and switching configurations. In order to simplify the analysis, it is assumed that at a given time, fault can occur in only one zone.

6.2 Verification and Analysis Results

We have used the PRISM model checker version 4.7 running on a Linux machine having specifications as core i5-7200 CPU at 2.71 GHz with 8.00 GB memory for the analysis. The relay failure, breaker failure, and communication failure probabilities are assumed to be 0.1, the probability of an error in the relay is also taken as 0.1. Moreover, we have assumed a

uniform probability distribution for the DG module, supervisory module, and CTM module. The verification is done for four zones-based PDN, as depicted in Fig. 6.1, with the conventional and auxiliary protection algorithms in place. The models are built and verified using the explicit engine of PRISM, which can efficiently handle the models with large state space, a fraction of which is reachable. The model building time for the traditional algorithm is 0.31 seconds, while the auxiliary algorithm took 1.87 seconds. To simplify the analysis, we have assumed that the "Trip Lockout" signal is always sent and received. The formal labels used for the verification of the reliability and safety of the traditional and auxiliary algorithms are presented in Listing 5. The PRISM properties and label details are listed below:

- `P=?[F "Isolation Success"]`: The label "Isolation Success" determines that after a fault in any zone, either the primary or backup breaker opens to isolate the faulty zone from the healthy zones.
- `P=?[F "Isolation Failure"]`: The label "Isolation Failure" indicates that after a fault both the primary and backup breakers are unable to isolate the faulty zone from the rest of the system.
- `P=?[F "False Trip"]`: The label "False Trip" occurs when CTM is less than 0.3 and the backup relay trips along with the primary relay, isolating the larger section from the healthy network.
- `P=?[F "Risk"]`: The label "Risk" indicates a protection concern. This occurs when $CTM > 0.4$ and after the t_p time has elapsed, the backup breaker is unable to isolate the faulty section, leaving the system exposed to the fault for a very long time.

With the help of the defined labels, the probabilistic verification over all scenarios is performed in all four zones of the PDN, and their results are discussed in detail in the following subsections.

Verification Results of Conventional Algorithm

The desired configuration scenarios when a fault occurs in zone Z1 are: (1) SC 3, SC 5, and (2) SC 1, SC 4. For these scenarios, here we provide the analysis for the conventional algorithm given in Fig. 5.1. In scenarios SC 3 or SC 5, if relay RA1 is in `Active` mode, then it acts as the PR, and if DG3 or DG4 is present, then relay RA2 is BR. First, the relay RA1 `Watchdog` module checks the relay for possible internal error, and then a *CTM* check is performed. Using the conventional algorithm, as shown in Fig. 5.1, *CTM* can lie in any one of the three possible

```
                ////  Traditional algorithm Properties   ////

label "Isolation Success"= ((B_p=1|B_b=1) & isol=true);

label "Isolation Failure"= (WD_p=1 & (RA_p=2|(RA_b=1 & B_b=3)))
       |(WD_p=2 & (((B_p=3 & B_b=3)|(RA_p=1 & B_p=3 & RA_b=2)
       |(RA_p=2 & B_b=3)|(B_p=2 & RA_b=2));

label "False Trip"= (CTM=2 & RA_p=1 & RA_b=1);

label "Risk"= (CTM=3 & RA_b=3 & t_b=true);

                /////  Auxiliary Algorithm Properties   /////

label "Isolation Success"= ((B_p=1|B_b=1) & isol=true);

label "Isolation Failure"= (WD_p=1 & B_b=3 & (s_p=3|s_p=4)))
       |((WD_p=2 & (CTM=2|CTM=3) & (RA_p=1 & BC_p=1 & B_p=3 & B_b=3)
       |(RA_p=1 & BC_p=2 & B_b=3)|(RA_p=2 & B_b=3));

label "False Trip"= (CTM=2 & (s_p=5|TL_Rb=2) & RA_p=1 & RA_b=1);

label "Risk"= (CTM=3 & sv_b=1 & t_b=true & BC_b=1 & B_b=3);
```

Listing 5: PRISM Labels of Protection System Properties

ranges, i.e., if the *CTM* is in the range 0.3<=CTM<=0.4 (i.e., CTM=1), then relay RA1 goes to `Operation` mode and issues a trip signal to breaker B1. If the fault is not cleared, then relay RA2 operates and trips breaker B2 to isolate the fault. However, if *CTM<0.3* (i.e., *CTM=2*), then relay RA2 may operate and trip breaker B1, along with the relay RA1, thus resulting in a false tripping action. But, if *CTM>0.4* (i.e., *CTM=3*) and relay RA1 or breaker B1 fails to operate and the operating time of relay RA2 exceeds the system threshold limit (*t_th*), then the system goes to the risk state. In SC 1 or SC 4, breaker B3 is closed, and relay RA2 protects zone Z1, here, relay RA3 acts as a BR. The chances of successful isolation of faulty section are 65.95%, whereas the chances of isolation failure are 4.06%, and the chances of false tripping are 24.30%. Moreover, there is a 5.69% chance of risk. The conventional algorithm operates in a similar manner for the rest of the three zones (Z2 to Z4) and corresponding scenarios, as discussed previously. If the system is in any of the desired configurations and a fault occurs in any of the four zones, the respective probabilities of the system to achieve "Isolation Success", "Isolation Failure", "False Trip", and "Risk" states are given in Table 6.2.

Table 6.2: Probabilistic Verification Results Conventional Algorithm

Fault Zones	Success	Failure	Risk	False Trip
Zone 1	0.6595	0.0406	0.0569	0.2430
Zone 2	0.6593	0.0406	0.0569	0.2430
Zone 3	0.6593	0.0406	0.0569	0.2430
Zone 4	0.6591	0.0407	0.0569	0.2430

Verification Results of Auxiliary Algorithm Part A

Case I-Fault in Zone Z1: The desired configuration scenarios when the fault occurs in zone Z1 are (1) SC 3, SC 5, and (2) SC 1, SC 4. We analyze the performance of the auxiliary algorithm Part A depicted in Fig. 5.2, for scenarios SC 3 or SC 5. Following the occurrence of a fault, if the relay agent RA1 is healthy and *CTM* is in range, then relays RA1 and RA2 undergo a normal operation. If *CTM* is not in range, then the relay RA1 issues a lockout command (*s_1=1*), sending the relay RA2 in the `Lockout` state. The relay RA1 then operates and sends a reset command (*s_1=2*) to release the relay RA2 from the `Lockout` state, followed by a trip signal to its associated breaker B1. If breaker B1 operates, then the fault is cleared successfully, and the system is said to be in an "Isolation Success" state. Otherwise, if the relay RA1 fails to issue a trip command to the breaker B1 or breaker B1 fails to operate, then relay RA1 sends a trip request command (*s_1=3*) to relay RA2 to clear the fault immediately. Similarly, if relay RA2 has an internal error, or it fails to receive the request signal (*TRQ_R2=2*), then the `Supervisory` module of the relay RA2 is activated after a predefined time delay, and it cancels all previous signals of the relay RA2 and issues a trip command to the breaker B2. If breaker B2 operates and the fault is cleared, then the "Isolation Success" state is achieved, otherwise, the system goes to the "Risk" state. With the auxiliary algorithm in place, the system either ends up in the "Isolation Success" state when the faulty zone is isolated or the "Isolation Failure" state when the fault is not isolated due to failure of relays or breakers, or the "Risk" state if the `Supervisory` service is activated and fault persists due to the failure of the backup breaker B2.

In scenarios SC 1 or SC 4, breaker B1 is open, so relay RA1 is out of service, relay RA2 acts as the PR and relay RA3 acts as BR, and the auxiliary algorithm performs in a similar manner as discussed above. Let us consider the case when relay RA2 is faulty, and it sends a trip request (*s_2=3*) to relay RA3 using the `Signal Dispatching` module. If the relay RA3 receives this

request command (*TRQ_R3=1*), it issues the trip command to breaker B3. If relay RA3 does not receive a signal (*TRQ_R3=2*) due to a communication failure, then its `Supervisory` module is activated after a predefined time and issues a trip command to the breaker B3. Moreover, there is a chance that relay RA2 is faulty, and at the same time, it is unable to issue a trip request (*s_2=4*) to relay RA3. In this situation, if relay RA3 is not stuck in the `Lockout` mode, then it will operate according to its setting. Otherwise, the `Supervisory` module is activated after a predefined period to clear the fault. Using the auxiliary algorithm for fault in zone Z1, the chances of "Isolation Success" are 96.25%, "Isolation Failure" are 3.44%, and the probability of the system going to the "Risk" is 0.31%. It is obvious from Table 6.3 that with the auxiliary algorithm Part A, the system either ends up in the "Isolation Success" when the fault zone is isolated or goes to the "Isolation Failure" or "Risk" state when the faulty zone is not isolated due to the failure of relays or breakers. However, there are no chances of "False Trip".

Case II-Fault in Zone Z2: The desired configuration scenarios for fault in Z2 are: (1) SC 3, SC 5, (2) SC 6, SC 10, SC 11, SC 12, and (3) SC 1, SC 4. In scenarios SC 3, SC 5, SC 6, SC 10, SC 11, and SC 12, relay RA2 is PR, and relay RA1 acts as a BR. To fully consider the impact of DGs penetration on the *CTM*, we assume that DGs are not present in the network. In this scenario, *CTM* is in range, and the relays RA2 and RA1 operate in a well-coordinated manner to isolate the fault. Thus, there is no need for an auxiliary algorithm, and the chances of the system reaching an "Isolation Success" state is 94.84%. Whereas the chances of "Isolation Failure" are found to be 5.15%. However, when DG1 and DG2 are connected to the network, their presence may disrupt the coordination between relays RA1 and RA2 causing *CTM* to go out of range, i.e., *CTM>0.4*. In this situation, if a fault occurs in zone Z2 while the relay settings are not updated, then the BR's operation time is very large, and if the PR fails to operate, the fault remains in the system for a long time. In such a condition, the line conductor may reach their thermal limits putting the system at risk. Without using the auxiliary algorithm, the chances of "Isolation Success" are 80.99%, "Isolation Failure" is 1.899%, and the chances of the system ending up in the "Risk" state are 17.10%. On the other hand, with the auxiliary algorithm in place, the chances of reaching an "Isolation Success" state are 96.25%, the likelihood of an "Isolation Failure" state is 3.44%, and the "Risk" state is 0.31%. Moreover, in SC 1 and SC 4, breaker B1 is open, and the relay RA1 is out of service. Considering DG1 or DG2 are connected, the relays RA2 and RA3 participate in the protection, and the verification results for the fault in zone Z2 considering all possible scenarios, are presented in Table 6.3.

Case III-Fault in Zone Z3: When a fault appears in zone Z3 then according to Table 6.1

Table 6.3: Probabilistic Analysis Results Auxiliary Algorithm

	Auxiliary Algorithm Part A				Auxiliary Algorithm Part B			
Fault Zones	Success	Failure	Risk	False Trip	Success	Failure	Risk	False Trip
Zone 1	0.9625	0.0344	0.0031	0.0	0.8966	0.0344	0.0031	0.0659
Zone 2	0.9625	0.0344	0.0031	0.0	0.8966	0.0344	0.0031	0.0659
Zone 3	0.9625	0.0344	0.0031	0.0	0.8966	0.0344	0.0031	0.0659
Zone 4	0.9586	0.0379	0.0035	0.0	0.8964	0.0370	0.0034	0.0632

the set of scenarios that can occur are: (1) SC 1, SC 4, and (2) SC 3, SC 5. In the first set of scenarios SC 1 and SC 4, breaker B1 is open while breaker SW is closed. The relay RA3 function as the PR, and if DG1 or DG2 is present, then relay RA2 supports as BR. However, in the second set of scenarios SC 3 and SC 5, relay RA2 will operate as the PR, and relay RA1 provides the required backup in the network. The verification results given in Table 6.3 show that the probabilities obtained in this case are the same as those obtained in the previous two cases.

Case IV-Fault in Zone Z4: The analysis of fault in zone Z4 is only possible if breaker B4 is closed. The list of possible configuration scenarios for zone Z4 are: (1) SC 1, (2) SC 3, and (3) SC 2, SC 6 to SC 9. In SC 3, the breaker B3 is open, breaker SW is closed, and the relay RA2 acts as a BR to relay RA4. Initially, let's consider the case when all DGs are connected to provide maximum power to the network. So, if the fault occurs in zone Z4, then the respective relays operate according to their defined settings. However, when DGs are disconnected from the network the relay, RA4, will experience a lower fault current. Therefore, the previous relay settings may not work. In this situation, the relays RA4 and RA2 experience the same fault current and $CTM < 0.3$. Now, the relay RA2 may operate before the relay RA4, causing the false tripping of the BR. Without using the auxiliary algorithm, the chances of "Isolation Success" are 21.95%, and of "Isolation Failure" are 5.15%, and the chance of "False Trip" is 72.90%. On the other hand, using the auxiliary algorithm, the relay RA4 sends the lockout command (*s_4=1*) to relay RA2 and operates according to its settings. During its `Operation` mode, it sends a reset signal (*s_4=2*) to relay RA2. If relay RA4 fails to operate, then it sends the trip request signal (*s_4=3*) to relay RA2. In case of communication failure between relays RA4 and RA2, after a specified time, the `Supervisory` module is activated to trip the breaker B2. In this way, the auxiliary algorithm successfully clears the fault without any maloperation. Moreover, the analysis results for fault in zone Z4 are given in Table 6.3.

Verification Results of Auxiliary Algorithm Part B

The above results were verified using Part A of the auxiliary algorithm. Part A assumes that the "Trip Lockout" signal is always sent and received and only examines the impact of "Trip Request" signal failure on the performance of the auxiliary algorithm. However, if $CTM < 0.3$ and communication between the PR and BR is disrupted, causing a loss of the "Trip Lockout" signal, the PR switches to `Operation` mode, and the unlocked BR may trip unnecessarily, causing false tripping, as shown in Part B of Fig. 5.2. The verification results using the Part B of the auxiliary algorithm are given in Table 6.3. It is obvious from these results that considering the failure of the "Trip Lockout" signal leads to the false tripping of BRs, resulting in non-zero "False Trip" probabilities.

Impact of Varying Communication Failure Probability on the Performance of Auxiliary Algorithm

The results presented in Table 6.3 are based on a fixed probability of communication failure of 0.1. However, in reality, the probability of communication failure can vary. Therefore, a rigorous analysis is performed by sweeping the communication failure probability from 0 to 1. The results depicted in Fig. 6.2, show that as the probability of communication failure for Part A increases from 0 to 1, the "Isolation Success" rate in zones Z1-Z3 decreases from 96.94% to 90.00%. As a result, the chances of "Isolation Failure" increase by 2.74%, lowering the overall system performance, and the chances of the system ending in the "Risk" state increases up to 4.20%. Furthermore, if a fault appears in zone Z4, the "Isolation Success" rate drops from 96.62% to 88.96%, resulting in an almost 7.66% reduction in "Isolation Success", and an increased level of "Isolation Failure", and "Risk" by 3.02%, and 4.64%, respectively. Finally, Fig. 6.3, provides the detailed results for Part B with varying levels of communication failure for all four zones.

Discussion

An auxiliary fault clearing d algorithm supporting the MAS-based schemes was first proposed in [8]. The ETAP simulation platform was used to analyze the protection coordination and total fault clearing times considering the three configuration scenarios only. The formal reliability and safety analysis has not been performed in that study. As fault clearing and communication failure have a significant impact on the system performance, our proposed methodology provides a rigorous analysis by considering all the possible switching configurations and

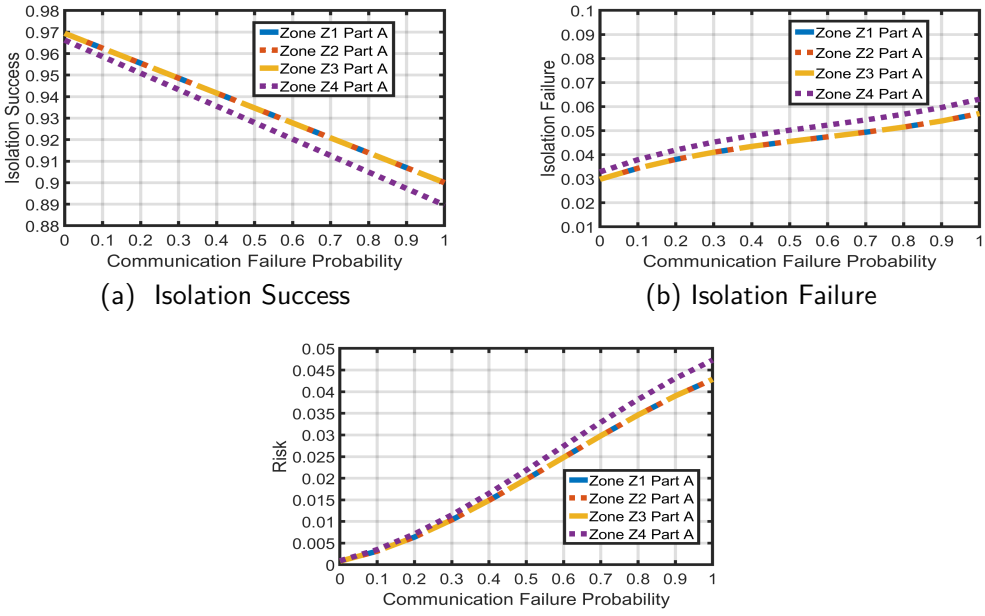

Figure 6.2: Impact of Varying Communication Failure Values on Aux. Algo. Part A (a) Isolation Success (b)Isolation Failure (c) Risk

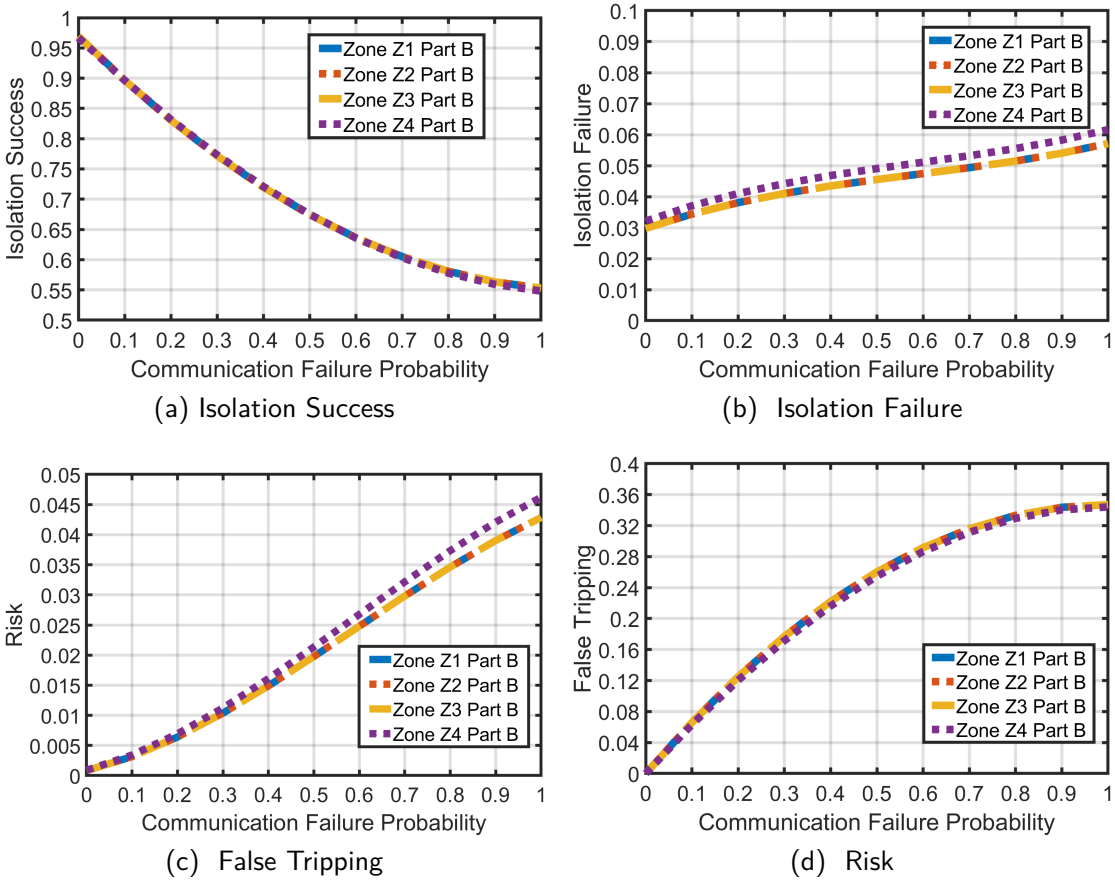

Figure 6.3: Impact of Varying Communication Failure Values on Aux. Algo. Part B (a) Isolation Success (b)Isolation Failure (c) False Tripping (d) Risk

DG penetration levels. Moreover, the formally verified safety properties can predict unforeseen issues in the protection of PDNs. For example, using the conventional algorithm, if a fault occurs in the PDN and the coordination margin is violated, then there are 5.6% chances that the system remains exposed to the fault for a longer time period and 24.3% chances of false tripping. False tripping of relays leads to the unnecessary isolation of a larger section of PDNs. The auxiliary algorithm uses a *Supervisory* module to isolate faults in the event of "Trip Request" signal failure or BR failure to prevent risk situations. However, if communication failure disrupts the "Trip Lockout" signal, the BR may malfunction, resulting in 6.5%, and 6.3% chances of false tripping. Thus, analyzing the impact of communication failure on the performance of the auxiliary protection algorithm highlights the need for more reliable communication. Given its rigorous nature, our formal analysis not only covers the scenarios, discussed in [8], but also includes all other possible network scenarios and the impact of "Trip Lockout" signal failure on the performance of the auxiliary algorithm, thus, allowing a more exhaustive analysis. This type of quantitative analysis helps engineers understand how well different protection algorithms can protect a PDN while maintaining reliability and safety.

Chapter 7

Conclusion

This study provides a framework for analyzing protection systems in PDN by developing behavioral models of protection system components, such as circuit breakers and digital relay agents, which are equipped with protection, signal dispatching, and auxiliary functionalities. This framework is utilized to analyze and compare the performance of a conventional and auxiliary fault-clearing algorithm supporting MAS-based schemes in emergencies, using the probabilistic model checker PRISM to verify its quantitative properties. A comparison of the conventional and auxiliary algorithms demonstrates the latter' s effectiveness in emergency scenarios. Moreover, the effect of communication failures on the performance of the auxiliary algorithm is also evaluated, which emphasizes the need for a more reliable communication network to prevent system failure and reduce undesired tripping scenarios. To the best of our knowledge, this is the first formal approach for verifying agent-based protection systems. In the future, we aim to provide a comprehensive formal framework for the reliability analysis of various MAS-based protection systems for fault isolation and service restoration by modeling different agents.

Bibliography

[1] S. Ashraf, I. Evkay, O. Hasan, U. S. Selamogullari, and M. Baysal, *Formal verification of single dual setting overcurrent directional relay based line protection logic for smart grids*, in 2021 3rd Global Power, Energy and Communication Conference (GPECOM), IEEE, 2021, pp. 227–232.

[2] S. Ashraf, I. Evkay, U. S. Selamogullari, M. Baysal, and O. Hasan, *Performance analysis of the dual-setting directional overcurrent relays-based protection considering the impact of curve types and fault location*, Electric Power Components and Systems, 51 (2023), pp. 706–723.

[3] S. Ashraf and O. Hasan, *Formal performance analysis of optimal relays-based protection scheme for automated distribution networks*, Engineering Science and Technology, an International Journal, 51 (2024), p. 101633.

[4] S. Ashraf, O. Hasan, I. Evkay, U. S. Selamogullari, and M. Baysal, *Recent trends and developments in protection systems for microgrids incorporating distributed generation*, Wiley Interdisciplinary Reviews: Energy and Environment, 13 (2024), p. e532.

[5] C. Baier and J.-P. Katoen, *Principles of model checking*, MIT press, 2008.

[6] J. Eto, *Blackout 2003: final report on the august 14, 2003 blackout in the United States and Canada: causes and recommendations*, Electricity Markets and Policy Group, Energy Analysis and Environmental Impacts Department, US Department of Energy, Washington, DC, (2004).

[7] I. Evkay, S. Ashraf, M. Baysal, U. S. Selamogullari, and O. Hasan, *Single dual setting directional over-current relay based line protection logic for dgs integrated power systems*, in 2020 2nd Global Power, Energy and Communication Conference (GPECOM), 2020, pp. 245–250.

[8] B. Fani, E. Abbaspour, and A. Karami-Horestani, *A fault-clearing algorithm supporting the mas-based protection schemes*, International Journal of Electrical Power & Energy Systems, 103 (2018), pp. 257–266.

[9] O. Hasan and S. Tahar, *Formal verification methods*, in Encyclopedia of Information Science and Technology, Third Edition, IGI Global, 2015, pp. 7162–7170.

[10] I. I. A. S. Industrial and C. P. S. Committee, *IEEE Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems: Approved September 19, 1985, Reaffirmed June 27, 1991 IEEE Standards Board: Approved February 28, 1986, Reaffirmed December 9, 1991, American National Standards Institute*, IEEE, 1986.

[11] B. Kasztenny, R. Hunt, and M. Vaziri, *Protection and control redundancy considerations in medium voltage distribution systems*, in 2007 60th Annual Conference for Protective Relay Engineers, IEEE, 2007, pp. 418–439.

[12] A. Khurram, H. Ali, A. Tariq, and O. Hasan, *Formal reliability analysis of protective relays in power distribution systems*, in International Workshop on Formal Methods for Industrial Critical Systems, Springer, 2013, pp. 169–183.

[13] M. Kwiatkowska, G. Norman, and D. Parker, *PRISM 4.0: Verification of probabilistic real-time systems*, in Proc. 23rd International Conference on Computer Aided Verification (CAV'11), vol. 6806 of LNCS, Springer, 2011, pp. 585–591.

[14] Z. Liu, C. Su, H. Høidalen, and Z. Chen, *A multiagent system-based protection and control scheme for distribution system with dgs integration*, IEEE transactions on power delivery, 32 (2016), pp. 536–545.

[15] A. Mahmood, O. Hasan, H. R. Gillani, Y. Saleem, and S. R. Hasan, *Formal reliability analysis of protective systems in smart grids*, in 2016 IEEE Region 10 Symposium (TENSYMP), IEEE, 2016, pp. 198–202.

[16] S. D. McArthur, E. M. Davidson, V. M. Catterson, A. L. Dimeas, N. D. Hatziargyriou, F. Ponci, and T. Funabashi, *Multi-agent systems for power engineering applications—part i: Concepts, approaches, and technical challenges*, IEEE Transactions on Power systems, 22 (2007), pp. 1743–1752.

[17] C. J. Mozina, *Impact of smart grids and green power generation on distribution systems*, IEEE Transactions on Industry Applications, 49 (2013), pp. 1079–1090.

[18] S. A. Naseem, R. Eslampanah, and R. Uddin, *Probability estimation for the fault detection and isolation of pmu-based transmission line system of smart grid*, in 2018 5th International Conference on Electrical and Electronic Engineering (ICEEE), IEEE, 2018, pp. 284–288.

[19] A. T. Nguyen, S. Reiter, and P. Rigo, *A review on simulation-based optimization methods*, Applied energy, 113 (2014), pp. 1043–1058.

[20] K. Pereira, B. R. Pereira, J. Contreras, and J. R. Mantovani, *A multiobjective optimization technique to develop protection systems of distribution networks with dgs*, IEEE Transactions on Power Systems, 33 (2018), pp. 7064–7075.

[21] D. Ranamuka, A. P. Agalgaonkar, and K. M. Muttaqi, *Examining the interactions between dg units and voltage regulating devices for effective voltage control*, IEEE Transactions on Industry Applications, 53 (2016), pp. 1485–1496.

[22] C. Su, Z. Liu, Z. Chen, and Y. Hu, *An adaptive control strategy of converter based dg to maintain protection coordination in distribution system*, in IEEE PES Innovative Smart Grid Technologies, IEEE, 2014, pp. 1–6.

[23] R. Uddin, S. A. Naseem, and Z. Iqbal, *Formal reliability analyses of plc network-based control in smart grid*, International Journal of Control, Automation and Systems, 17 (2019), pp. 3047–3057.

[24] K. A. Wheeler, M. Elsamahy, and S. O. Faried, *A novel reclosing scheme for mitigation of dgs effects on overcurrent protection*, IEEE Transactions on Power Delivery, 33 (2017), pp. 981–991.