

ORIGINAL ARTICLE

Enhanced Adaptive Overcurrent Protection Scheme for AC Microgrid and Its Real-Time Validation Through Cyber Physical Power System Testbed

Amar Jagan  | Udit Prasad  | Soumya R. Mohanty  | Shiv P. Singh 

Department of Electrical Engineering, Indian Institute of Technology (BHU) Varanasi, Varanasi, Uttar Pradesh, India

Correspondence: Udit Prasad (uditprasad.rs.eee19@iitbhu.ac.in)

Received: 17 May 2024 | **Revised:** 3 January 2025 | **Accepted:** 23 February 2025

Funding: The authors acknowledge the support from the Science and Engineering Research Board (SERB), Department of Science and Technology (DST), Government of India, under the scheme CRG/2020/005716, and the Central Power Research Institute (CPRI), Bangalore, Ministry of Power, Government of India (Grant No. : CPRI/R&D/TC/Trans/2022) to carry out this research work.

Keywords: cyber-physical testbed | HIL | IEC 61850 | microgrid protection

ABSTRACT

This paper introduces a Relay Integrity and Anomaly Detection (RIAD) scheme designed to enhance the reliability of Setting Group-based Adaptive Overcurrent (SGAO) protection systems. The RIAD mechanism improves relay configuration awareness and mitigates potential failures due to misconfigured relays or cyber intrusions targeting relay settings. To validate the performance of SGAO and the proposed RIAD, a comprehensive cyber-physical power system testbed was developed and implemented within the CIGRE 7-bus AC microgrid. This field-level testbed, featuring IEC 61850-based Hardware-in-the-Loop (HIL) experimentation with Real-time Digital Simulation (RTDS) and industry-grade relays such as SEL 421, 751, and 311C, along with an automation controller (SEL RTAC 3530-4) for logic implementation, provides a precise timeline analysis of events. The testbed highlights the significance of validating enhanced SGAO schemes under real-world conditions, ensuring robust relay settings and coordination even in the presence of communication failures, misconfigurations, or cyber-attacks.

1 | Introduction

Conventional power system protection schemes are often inadequate in effectively addressing the unique challenges presented by microgrid systems, which involve bidirectional power flow and diverse network configurations. The variability of fault currents across different configurations exacerbates the issue and compromises the effectiveness of overcurrent (OC)-based protection coordination. To address these challenges, researchers have proposed adaptive OC protection schemes based on relay setting groups (SGs). In standard SG-based protection schemes, the active setting within a predetermined SGs is selected based on the prevailing operating conditions of

the microgrid. These conditions include the mode of operation (e.g., grid-connected or islanded), network topology, distributed generator (DG) integration, and other pertinent factors. The literature emphasizes methods and techniques for determining these relay settings optimally, with a focus on ensuring proper coordination between the relays. This optimization aims to minimize the overall operating time, reduce the computational complexity involved in calculating these settings, and accommodate various operating conditions as previously mentioned. An OC protection scheme for dual-setting directional OC relays is proposed in [1], considering the limitations on the number of SGs in such relays. In [2], the relay coordination objective function is revised to incorporate N-1

Amar Jagan and Udit Prasad are co-first authors with equal contributions.

contingency considerations. The influence of interconnected transmission networks on microgrids, along with their inherent uncertainties, is addressed in [3]. Further, [4] employs a hybrid Artificial Neural Network (ANN) and Support Vector Machine (SVM) approach for improved topology identification, facilitating the deployment of an SG-based OC protection scheme. Notably, the power network models utilized in these studies are developed using DigSILENT Power Factory for data extraction, while MATLAB serves as the central platform for algorithm implementation and operation execution. However, there is minimal focus on the communication infrastructure required for relay SG updates and event timeline.

Adaptive protection schemes in the literature primarily focus on assessing technique performance under various operating conditions. Notably, [5] integrates GAMS, AMPL, and MATLAB to develop adaptive OC protection strategies, accommodating scenarios such as load loss, line generation, and relay miscoordination induced by DG injections. Constraint Reduction Method was proposed to reduce the complexity and enhance the performance of adaptive protection systems, amidst varying DG sizes, locations, and system configurations [6]. Studies [7, 8] introduced robust numerical relays designed using fast recursive discrete Fourier transform and fuzzy logic decision-making modules and a differential evolution algorithm, respectively. Additionally, [9] employed a Mixed-Integer Linear Programming (MILP) method to determine optimal relay settings. The protection of networked microgrids was addressed in [10], where a nonlinear programming-based algorithm, along with k-means clustering, was utilized to categorize optimal relay settings for different network topologies. Despite the comprehensive discussions on the proposed schemes [5, 8–10], there remains a gap in the actual integration of communication system. Such integration is crucial for facilitating real-time analysis of event timelines and updating relay settings. These schemes rely on a centralized MATLAB platform, with the assumption of dependence on the communication system for retrieving system states and updating relay settings.

In order to assess the feasibility of adaptive OC protection schemes in practical applications, several studies have utilized real-time simulation platforms for verification purposes. In [11–13], Real-Time Digital Simulator (RTDS)-based Hardware-in-the-Loop (HIL) setup is employed, with [11] focusing on the coordination of OC relays in AC microgrids and [12] exploring optimal OC relay settings in multimicrogrids with fault current limiters. In [13], a Programmable Logic Controller (PLC) is utilized for implementing SG changes. However, it remains unclear whether communication protocols were employed in the HIL setup for information exchange among the hardware components. Further, [14] conducted real-time analysis using an OPAL-RT platform with a digital relay, while [15] validated an SG-based OC protection scheme on an RTDS platform with a Numerical Relay Development Environment (NRDE) [16], noting backup provisions for communication failures. However, the communication aspects of the microgrid were not addressed during HIL verification. An OC protection scheme for wind farms employing gray wolf optimization and a fuzzy logic controller was introduced in [17], with implementation on a Field Programmable Gate Arrays (FPGA) board and MATLAB integration. Basic adaptive OC protection schemes were examined

in [18] and [19] using RTDS-based and OPAL-RT-based HIL setups, respectively, incorporating digital relays to assess feasibility. Notably, [18] included a PC with DNP3 and IEC 61850 GOOSE communication, representing a cyber-physical system. The validation of SG-based adaptive OC (SGAO) protection schemes with a focus on both cyber and physical domains of power systems was the core of [20, 21], with [21] employing an IEC 61850-based testbed and industrial relays. The verification and analysis techniques used in these works are summarized in Table 1. However, adaptive protection schemes in the literature often overlook critical aspects, such as relay misconfiguration. Additionally, the application of IEC 61850 GOOSE in controlling SGs [6, 9, 11, 15, 18, 20, 21] introduces vulnerability to cyber-attacks [32].

Numerous studies have explored cyber-attacks on protection systems, including false data injection on line current differential relays [25–26], transmission line protection compromise [28, 29], stealthy transformer tap manipulation [27], distance protection and circuit breaker control breaches [30], attack targeting breaker failure protection [31], and synchronization disruption in synchronous generator [33]. However, the literature lacks an examination of relay misconfiguration within adaptive protection schemes, a potentially critical vulnerability to cyber-attacks altering relay SGs stealthily. The consequence of such cyber-attacks could manifest as either an unintended or false trip of circuit breakers during non fault periods, or conversely, a failure of circuit breakers to trip during actual faults. These scenarios may lead to significant repercussions such as increased load shedding, or in extreme cases, endangering customer safety.

This research paper addresses the limitations in analyzing and implementing SGAO protection schemes with optimal relay settings for relay coordination through a near-practical field-level cyber-physical testing environment. With the increasing reliance on communication networks in modern power systems, the paper primarily focuses on addressing relay misconfiguration caused by cyber intrusions through the proposed Relay Integrity and Anomaly Detection (RIAD) scheme. Additionally, high-precision experimentation, including the operation of SGAO integrated with the RIAD and its response to cyber intrusions, provides critical insights for the successful implementation of protection schemes in practical applications. This comprehensive analysis enables a deeper understanding of protection schemes, facilitating informed decision-making and improving reliability in real-world scenarios.

To this end, the paper makes the following contributions:

1. Development of a specialized field-level cyber-physical power system testbed based on the IEC 61850 substation protocol, specifically designed for the analysis of the proposed SGAO protection schemes.
2. Implementation of hardware synchronization using an industrial satellite clock to ensure precise timeline analysis of protection and anomaly events, enabling analysis at the nanosecond level.
3. Incorporation of a data packet modifier in the network domain to assess the impact of deliberate cyber intrusions on the performance of the protection system.

TABLE 1 | Verification and analysis techniques.

Reference	Tools	Real-time	HIL	Cyber-physical	Time sync.	Cyber-intrusion	Relay SG-misconfig.
[1–4]	A, B	—	—	—	—	—	—
[6, 7, 9, 22, 23]	B	—	—	—	—	—	—
[5]	B, AMPL, GAMS	—	—	—	—	—	—
[17]	B, FPGA	*	✓	—	—	—	—
[11, 12]	D, E	✓	✓	—	—	—	—
[15]	D, NRDE [16]	✓	✓	—	—	—	—
[19]	C, E	✓	✓	—	—	—	—
[13]	D, E, PLC	✓	✓	*	—	—	—
[14]	C, E	✓	✓	*	—	—	—
[18, 20]	D, E	✓	✓	✓	—	—	—
[21]	C, E	✓	✓	✓	—	—	—
[24]	C	✓	✓	—	—	✓	—
[25, 26]	PSCAD/EMTDC	—	—	—	—	✓	—
[27]	B	—	—	—	—	✓	—
[28]	C—HYPERSIM	—	—	—	—	✓	—
[29, 30]	D, E	✓	✓	✓	✓	✓	—
[31]	PSCAD/EMTDC	✓	✓	✓	✓	✓	—
Proposed	D, E, MG Controller, Satellite Clock	✓	✓	✓	✓	✓	✓

Note: *not mentioned, **A**: DIgSILENT **B**: MATLAB/SIMULINK, **C**: OPAL-RT, **D**: RTDS, **E**: Digital Relay

- Introduction of an anomaly detection mechanism, RIAD, designed using logic compliant with the IEC 61131-3 standard, to inspect relay misconfigurations within the SGAO protection schemes.

Through these contributions, the paper aims to enhance the reliability of protection schemes for modern power systems, offering valuable insights for their practical implementation in field scenarios. Monitoring relay settings via predictive alarming gives engineers the necessary data to keep power system protection components online and avoid expensive downtime. This paper utilizes the SEL Real-Time Automation Controller (RTAC) to build an automated RIAD mechanism to continuously monitor and validate many of the components identified in the NERC PRC-005 standard, including verification of commissioned intelligent electronic devices (IED) settings and communication-assisted protection channel integrity.

The remaining sections of this paper are structured as follows. Section 2 provides an overview of the SGAO protection scheme with optimal relay settings for relay coordination and RIAD mechanism for reliable protection operation. In Section 3, we present a detailed description of the developed cyber-physical power system testbed. Section 4 discusses the implementation

of the SGAO scheme, integrated with the RIAD mechanism, within the proposed testbed. The results, including analysis of various protection actions and responses to cyber intrusions, are presented in Section 5. Finally, Section 6 concludes the paper and summarizes the key findings.

2 | Enhanced Adaptive OC Protection Through Relay SG Awareness Mechanism

The Federal Energy Regulatory Commission (FERC) oversees the North American Electric Reliability Corporation (NERC), which is tasked with enhancing the reliability of the bulk electric system (BES) in North America. Protective relays and the associated communication systems fall under the definition of protection systems as outlined in NERC PRC-005-2, which is updated to adapt to new and evolving protection system components. Adhering to this standard necessitates developing a thorough protection system maintenance program and carrying out maintenance activities on a regular basis. By leveraging the inherent functionality of the proposed RIAD mechanism and the communication capabilities of modern IEDs, an automated system can be implemented by engineers to enable real-time monitoring, validation, and reporting of

power system components. This approach provides improved protection system awareness, detects improperly configured IED settings that could otherwise remain undetected, and facilitates the maintenance and validation testing processes for all monitored critical protection relays. Additionally, it can document the behavior of power system components during fault events and cyber anomalies under different operational and topological conditions. The RTAC is used to build an automated RIAD mechanism that continuously monitors and validates commissioned IED settings and the integrity of communication-assisted protection channels.

2.1 | Introduction: Test System and Its Associated Protection Scheme

The 7-bus AC microgrid system in Figure 1 is used to demonstrate and validate the features and capabilities of the adaptive protection scheme and the proposed RIAD mechanism using the developed cyber-physical testbed [15, 34]. The microgrid with a nominal voltage of 13.2kV and frequency 60Hz is connected with a utility grid with a nominal voltage of 138kV through a transformer and the switch S1 at the point of common coupling (PCC) facilitates this connection. In the 7-bus system, there are three DGs incorporated out of which 1.74 MW PV source at Bus 3 and 2 MW wind energy source at Bus 5 are inverter interfaced and a 5.5 MVA diesel generator at Bus 7 is synchronous machine based. In the event of islanding, the diesel generator stabilized the system voltage and frequency.

With the operation of S1, SW1, and SW2, the system can take four major operating modes based on whether the system is grid connected (GC) or islanded (IM) and whether the system is in mesh or radial configuration. Table 6 lists the different operating modes of the system, namely, Grid Connected Mesh (GCM), Islanded Mesh (IMM), Grid Connected Radial (GCR), and Islanded Radial (IMR). The incorporated test system accurately captures challenges such as fault current variability, modes of operation, and network topology, which commonly arise in actual AC microgrids with multiple generation sources.

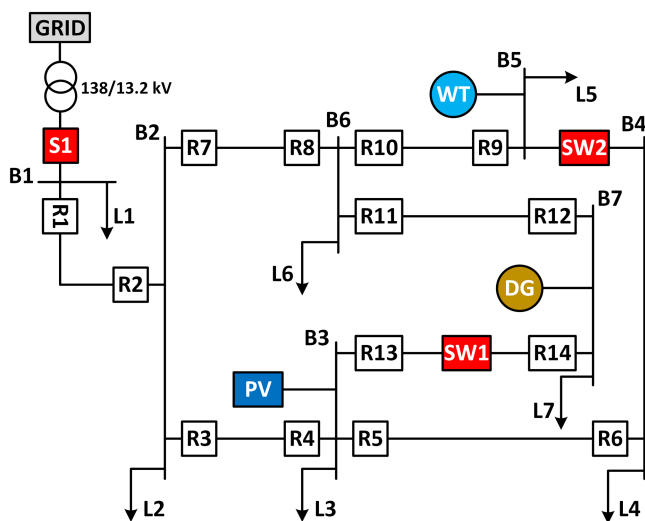


FIGURE 1 | The 7-bus AC microgrid test system.

By reflecting practical scenarios, it demonstrates the system's effectiveness in a comprehensive context, thereby validating its performance in realistic applications. For each mode, the table also specifies the status of switches in the network and the corresponding relay word bits, referred to as virtual bits, which are necessary to control the SG state. SGs are predefined configurations within the numerical relays that change according to operating conditions [35].

Directional OC relays are installed at both ends of each feeder in the network. In a mesh system, a total of 14 relays are operational, whereas in a radial system, Relays 13 and 14 remain inactive as the associated line is not engaged. The Current Transformer Ratio (CTR) of each relay is computed by considering the maximum fault current and maximum load current for all feasible configurations [10, 36, 37], as described in the following equation:

$$CTR_n = \max\left(I_{L,max,n}^i, \frac{1}{20}I_{f,max,n}^i\right) \quad (1)$$

where n is the relay number and i are different network configurations possible. This equation ensures that the current transformer (CT) ratio (CTR) is capable of handling the greater of either the maximum load current $I_{L,max,n}^i$ or the adjusted maximum fault current $\frac{1}{20}I_{f,max,n}^i$, without causing saturation. The division of the maximum fault current by 20, which represents the Accuracy Limit Factor (ALF) or the rated accuracy limit current, is based on standards specified by IEEE C57.13 and IEC 60044-1 for CTs of the C100 and 5P20 classes, respectively. These CT classes are designed for OC relays in protection applications, particularly for feeder protection. The standards ensure that the CT operates accurately under both load and fault conditions without exceeding acceptable limits. Saturation occurs when the magnetic core of the current transformer is subjected to excessively high current, resulting in a nonlinear response that produces a distorted output signal. This distortion can lead to inaccurate current measurements and compromised protection system performance. Thus, this is critical for maintaining the accuracy and reliability of current measurement and protection relay operation. For consistency, a secondary current of 1 A is considered for the CTs, and the CTR values are selected as multiples of 100. The primary and backup relay (PR and BR) pairs are obtained using LINKNET structure based algorithm [11, 38] where the network connection details are fed to obtain the PR and BR pairing. The CT ratios for each relay and the corresponding PR-BR combinations for all four operating modes of the 7-bus microgrid are given shown in Table 2.

Furthermore, SGAO is enhanced by integrating a group awareness mechanism to mitigate potential vulnerabilities. Conventional protection schemes rely on relays configured with the assumption that control commands for SG changes from the microgrid controller are authentic. Failure to authenticate these commands can result in cascading system outages, leading to increased customer load shedding. In the worst-case scenario, this failure may result in a complete blackout. Conversely, the system may fail to respond to faults, posing a significant risk to both line workers and customers.

TABLE 2 | CTR and PR-BR pairing for the relays.

PR	CTR	Mesh		Radial	
		BR1	BR2	BR1	BR2
R1	800	—	—	—	—
R2	100	R8	R4	R8	R4
R3	200	R8	R1	R8	R1
R4	100	R14	R6	R6	—
R5	200	R14	R3	R3	—
R6	100	R10	—	—	—
R7	200	R4	R1	R4	R1
R8	200	R12	R9	R12	R9
R9	100	R5	—	—	—
R10	200	R12	R7	R12	R7
R11	200	R9	R7	R9	R7
R12	200	R13	—	—	—
R13	200	R12	R3	—	—
R14	200	R11	—	—	—

2.2 | Conventional SG-Based Adaptive Protection and Protection Coordination

The adaptive protection scheme employed in the test AC microgrid is a widely accepted approach designed to account for varying operational conditions, such as grid-connected and islanded modes of operation, as well as radial and meshed network topologies with dynamically changing fault current levels. Adaptive protection enables real-time adjustments to the SGs of the protective IEDs by utilizing switch status information from S1, SW1, and SW2 to determine the system's operational mode, as outlined in 6. This approach enhances the network's reliability and resilience under these operating conditions, preventing unnecessary or missed tripping during diverse fault scenarios [10, 11, 39]. The flowchart illustrating the adaptive OC protection scheme is depicted in Figure 2. To determine the optimal relay settings for each operating mode, a combination of DlgSILENT Power Factory and MATLAB is utilized which is a commonly employed offline technique in the literature [1–3, 40].

In the adaptive OC protection scheme, the determination of PR-BR pairs for each operating mode is initiated by employing the LINKNET structure-based algorithm. Subsequently, a load flow analysis is conducted to ascertain the maximum load current ($I_{L,max}$), while a short circuit analysis is performed to obtain the minimum fault current ($I_{f,min}$) by applying the least severe fault at the far end of the line, as well as the maximum fault current ($I_{f,max}$) by applying the most severe fault at the near end of the line. The fault currents at the corresponding backup relays are also recorded during this analysis. These collected data are then utilized to solve an optimization problem aimed at determining the optimal relay settings. The obtained relay settings are subsequently stored in the corresponding SGs within the digital relays.

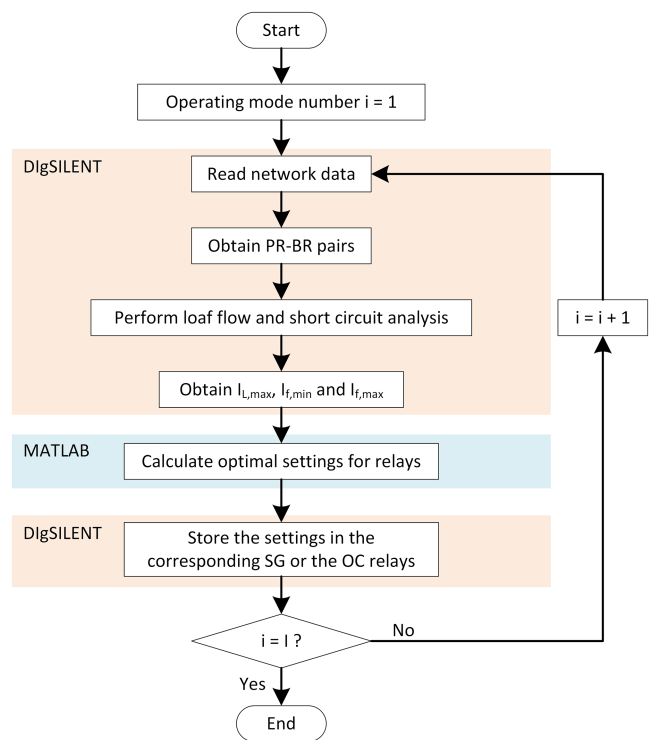


FIGURE 2 | The process for finding optimal relay settings.

2.3 | Calculation of Optimal Relay Settings

The relay setting optimization problem is formulated to determine the optimal values for the Pickup Setting (PS) and Time Dial Setting (TDS) of the relays. The objective is to minimize the total operating time of the relays, taking into account both the primary relays (PR) and their corresponding backup relays (BR). The optimization problem can be defined as follows:

$$\min \left(\sum_{n=1}^N t_{PR,n} + \left(\sum_{m=1}^M t_{BR,m} \right) \right) \quad (2)$$

where

$$t_n = TDS_n \times \frac{0.14}{\left(\frac{I_f}{PS_n} \right)^{0.02} - 1} \quad (3)$$

s.t.,

$$PS_{min,n} \leq PS_n \leq PS_{max,n} \quad (4)$$

$$TDS_{min} \leq TDS_n \leq TDS_{max} \quad (5)$$

$$t_{PR,min} \leq t_{PR,n} \leq t_{PR,max} \quad (6)$$

$$t_{BR,m} - t_{PR,n} = MTI \quad (7)$$

Equation (2) represents the objective function (OF) of the optimization problem. In this equation, $t_{PR,n}$ denotes the operating time of the “n-th” primary relay when a three-phase fault occurs at the near end of the line. Similarly, $t_{BR,m}$ represents the operating time of the “m-th” backup relay (BR) associated with the PR for

the same fault scenario. “N” represents the total number of relays, while “M” indicates the number of BRs backing up the “n-th” PR.

The relay operating time is determined using the standard inverse curve specified in IEC 60255, as defined in (3). This equation incorporates the OF variables, namely, PS_n (Pickup Setting) and TDS_n (Time Dial Setting), which introduce non-linearity to the function.

Among the four constraints applied to the optimization problem, (4) and (5) serve as boundary constraints for the variables. In these equations, and $PS_{min,n}$ and $PS_{max,n}$ represent the lower and upper bounds, respectively, for the pickup setting of the “n-th” relay. Similarly, TDS_{min} and TDS_{max} establish the lower and upper bounds applicable to all relays. These bounds are determined based on specific criteria. To ensure selectivity of the relays between overloaded situations and minimum fault conditions, the value of PS_{min} is set to 1.5 times the maximum load current ($I_{L,max}$). Furthermore, to ensure that the relays remain sensitive to the minimum fault under consideration, PS_{max} is set to 0.66 times the minimum fault current ($I_{f,min}$) [11, 15, 41–43]. The range of TDS values depends on the relay operating curve, and for this study, the lower and upper bounds of 0.05 and 5 s, respectively, have been chosen for TDS.

Equations (6) and (7) represent nonlinear constraints in the optimization problem. The operating time of the primary relay (PR) for a fault within its zone is bounded by $t_{PR,min}$ and $t_{PR,max}$, which are specified as 0.2 and 2 s, respectively. These settings were chosen based on standard relay coordination practices to ensure a minimum operating time while preventing excessive delays in the relay’s response to a fault [11, 41]. The constraint in (7) ensures a minimum time interval (MTI) for the operation of the backup relay (BR), thereby ensuring proper relay coordination.

The nonlinear optimization problem is solved in the MATLAB environment (Figure 2) using the Sequential Quadratic Programming (SQP) method. The obtained relay settings are presented in Table 3.

2.4 | Relay Integrity and Anomaly Detection Scheme

This section outlines the proposed RIAD scheme aimed at enhancing the robustness of centralized SGAO protection schemes. This entails the implementation of a comprehensive real-time maintenance scheme, potentially leveraging centralized automated monitoring and logical systems compliant with the IEC 61850 and IEC 61131-3 standards. Traditional SGAO protection schemes operate under the presumption that the SGs are authentic. This framework seeks to augment relay configuration awareness and mitigate potential relay failures stemming from misconfigurations or cyber intrusions targeting SGs. This approach facilitates the prevention of downtime and enables predictive maintenance. The scheme relies on the utilization of the SEL 3530-4 RTAC to monitor and validate critical settings and assess communication integrity. The integration of these measures significantly improves the reliability and effectiveness of SGAO.

The proposed RIAD scheme relies on feedback signals, carrying the active SG status, transmitted by the connected relays compliant with the GOOSE protocol, as depicted in Figure 3. These signals are dispatched at the prevailing GOOSE broadcasting rate within the system, which offers multiple advantages:

- Communication efficiency: Reducing communication traffic, mitigating network congestion and ensuring that other systems remain responsive and efficient.

TABLE 3 | Optimal relay settings for different operating modes.

PR	GCM		IMM		GCR		IMR	
	PS	TDS	PS	TDS	PS	TDS	PS	TDS
R1	0.706	0.092	—	—	1.295	0.089	—	—
R2	1.400	0.077	2.070	0.064	0.361	0.066	0.453	0.061
R3	4.279	0.05	0.774	0.134	1.303	0.05	0.639	0.05
R4	5.723	0.05	1.328	0.05	0.761	0.097	0.100	0.056
R5	2.695	0.053	0.668	0.076	1.024	0.055	0.307	0.072
R6	1.509	0.075	1.400	0.150	—	—	—	—
R7	3.380	0.05	1.51	0.128	1.569	0.051	1.493	0.05
R8	1.340	0.059	0.361	0.089	1.559	0.052	1.742	0.05
R9	2.985	0.053	0.585	0.054	0.168	0.105	0.207	0.086
R10	3.024	0.05	2.740	0.090	0.808	0.059	0.487	0.053
R11	1.711	0.055	0.693	0.321	0.308	0.080	0.526	0.05
R12	2.838	0.05	1.042	0.675	1.387	0.05	1.521	0.05
R13	3.760	0.05	1.012	0.683				
R14	3.245	0.05	0.986	0.283				

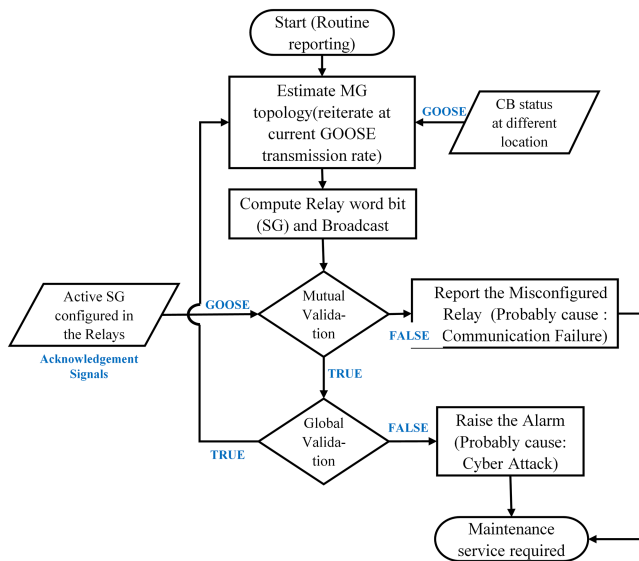


FIGURE 3 | Process flow for relay configuration validation.

- **Bandwidth conservation:** Messages are transmitted as necessary to preserve communication integrity, rather than incessantly, thereby saving bandwidth.
- **Priority handling:** Critical events receive prioritized transmission, ensuring lower latency crucial for real-time operations of the proposed RIAD scheme.
- **Real-time data delivery:** Ensuring that relevant data are delivered to the centralized controller (RTAC) with minimal delay, determined by the quality of the communication system.

The verification process consists of two stages: mutual validation and global validation, as shown in Figure 3. Mutual validation ensures that all relays are configured with the same SG, triggering an alarm if discrepancies in active settings are identified, thereby identifying the misconfigured relay. Conversely, global validation ensures that relay settings align with the actual network topology. Potential failures in mutual validation may stem from faults, attacks, or communication breakdowns within individual relays, whereas global validation failures could result from cyber-attacks targeting communication channels transmitting SGs control commands. It is assumed that attackers possess knowledge of the power system and communication infrastructure, enabling stealthy and strategic manipulation of actual control commands received by relays. However, it is worth mentioning that deviations from preset logic prompt default SG activation (i.e., SG1), mitigating potential risks.

3 | Cyber-Physical Testbed

The cyber-physical power system testbed presented in this study is built using the RTDS platform and incorporates industrial relays, a microgrid controller, and a satellite clock. Figure 4 illustrates the connection diagram, and Figure 5 showcases the laboratory setup of the HIL testbed. Table 4 presents a list of the hardware tools employed in the development of the proposed cyber-physical testbed, along with their respective purposes.

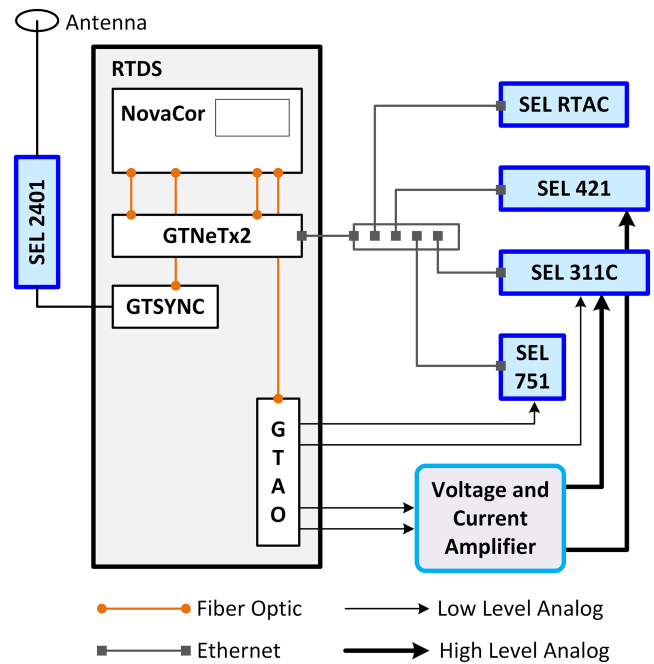


FIGURE 4 | Diagram of cyber-physical testbed showing means of interconnection of equipment.

Additionally, Table 5 lists the software tools employed and provides an overview of their roles in the development process.

3.1 | RTDS and Interfacing

A real-time simulation platform based on RTDS is utilized for simulating the power network within the testbed. This platform offers various options for interfacing with external devices. The GTA0 card, an analog signal interface card, is employed to provide the required bus voltage and line current signals for the relays. The GTA0 card enables the provision of low-level analog signals within the $\pm 10V$ range. To facilitate communication network-based interfacing, the RTDS system incorporates the GTNETx2 card, which supports multiple network communication protocols. In this testbed, the GTNETx2 card is utilized for implementing the GOOSE protocol.

3.2 | Relays and Microgrid Controller

The industrial numerical relays are employed in the HIL experiments within the testbed to ensure a close representation of real-world field setups. This facilitates the seamless implementation of developed protection schemes once they have been verified. Although the relays SEL 421, SEL 751, and SEL 311C used in the testbed serves specific purposes, all of them incorporate sufficient protection elements for effective application in distribution system OC protection. To amplify the low-level analog signals from the GTA0 card to levels compatible with the back panel input of the relays, a voltage and current amplifier is employed. Given the limitation in the number of output channels in the amplifier, high-level signals are directed to the SEL 421 relay, while the remaining relays are operated through the low-level test interface.

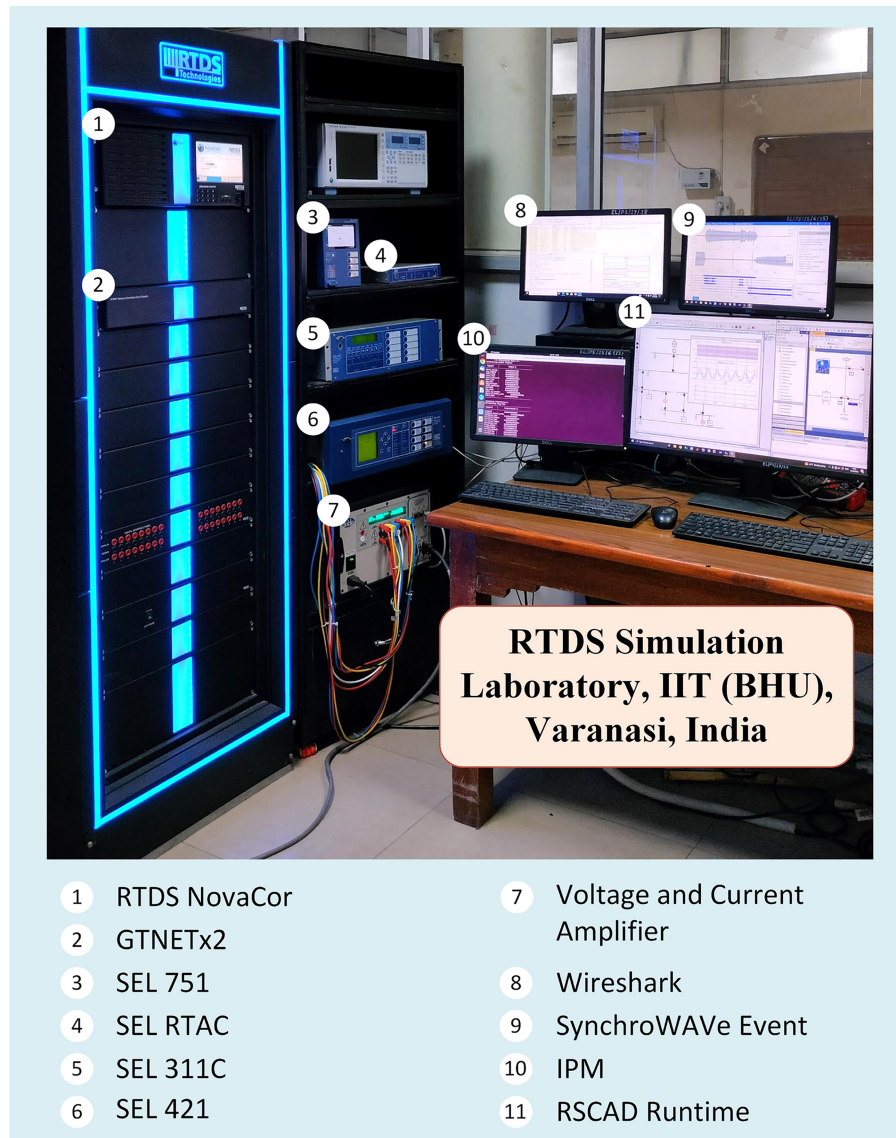


FIGURE 5 | Laboratory setup of cyber-physical testbed showing major equipment and software used.

To implement centralized SG change logic and RIAD mechanism, a SEL RTAC 3530-4 microgrid controller is integrated into the testbed. The RTAC serves as a data concentrator and communication gateway, featuring an integrated IEC 61131 programming environment for executing control logic and algorithms using industry-standard languages like Continuous Function Chart (CFC) and Structured Text (ST). It also supports GOOSE communication. Leveraging these capabilities, the RIAD mechanism monitors and validates IED SGs in substations, simplifying power system maintenance across various substation topologies. RIAD outputs include SG control commands as virtual bits and Boolean alerts, providing status information on connected relays. Communication protocols are configured in acSELeRator RTAC to retrieve relay SG status points at GOOSE transmission rates, feeding them into function block inputs for processing. These inputs are monitored for significant status mismatches based on user-specified logic, with outputs stored in a virtual tag list for post-analysis.

3.3 | Time Synchronization

Ensuring synchronized timesteps across all devices within the cyber-physical testbed is crucial for accurate analysis of fault scenarios and protective action. To achieve this, both the RTDS system and external devices in the testbed are synchronized to a common timestamp using signals received from GPS satellites. This synchronization process is implemented through the utilization of a satellite-synchronized clock, specifically the SEL 2401, along with an antenna. The clock's signal is distributed to both the external hardware and the RTDS system. Within the RTDS system, the GTSYNC card facilitates the synchronization of the power network simulation.

3.4 | Inline Packet Modifier

In this work, an Inline Packet Modifier (IPM) is employed to simulate cyber intrusions in the communication channel

TABLE 4 | List of major hardware in cyber-physical testbed.

Hardware	Description	Application
RTDS NovaCor	Real time simulation platform	Power network simulation
GTAO	Analog signal interface card	Provide three phase bus voltage and line current to relays
GTNETx2	Network interface card	Facilitate GOOSE communication
GTSYNC	Time synchronization card	Synchronise RTDS simulation time with GPS clock
SEL 421, SEL 751, SEL 311C	Numerical relays	Perform HIL with RTDS to verify protection algorithm
F6350e	Voltage and current amplifier	Amplify low level analog signals from RTDS to high level voltage and current signals for relays
SEL RTAC	Microgrid controller	Run setting group (SG) change algorithm
SEL 2401, Antenna	Satellite clock and antenna	Synchronise external hardware and RTDS with GPS clock

TABLE 5 | List of software for testbed implementation.

Software	Application
RSCADfx	Build power network for microgrid
RSCAD runtime	Real-time monitoring and control of power network
ICT	Configure GOOSE for IEDs in RSCADfx
AcSElerator Quickset	Configure relays, monitor measurements and record events
SynchroWAVE Event	Visualize and analyze recorded events from relays
AcSElerator RTAC	Implement SG change algorithm in RTAC
AcSElerator Architect	Configure GOOSE for SEL based IEDs
F6 Multiple Amplifier Configurator	Configure amplifier
Wireshark	Analyze GOOSE packets

using a dedicated Linux-based system [44]. The IPM integrates features from two Linux open-source tools: SNORT and Linux Traffic Control (TC). SNORT, an open-source Intrusion Prevention Software (IPS) owned by Cisco, is widely recognized for its protocol analysis and detection of attacks such as buffer overflows and Common Gateway Interface (CGI) attacks. Within the IPM framework, SNORT is customized to process data packets for various substation communication protocols; however, in our application, it is specifically utilized for GOOSE packets.

Within the Linux-based system, data packets enter the kernel through a Network Interface Card (NIC), as shown in Figure 6.

A NIC with four Ethernet ports (enp6s0, enp7s0, enp8s0, and enp9s0) is installed to support this setup. As data packets enter through enp6s0, they undergo filtering and are subsequently placed into ingress queues. Similarly, before exiting via enp9s0, the packets join egress queues. As illustrated in the figure, SNORT operates between interfaces enp6s0 and enp7s0, while TC runs between enp8s0 and enp9s0. These pairs of interfaces are physically connected externally via Ethernet, while each pair is bridged internally through software. Since communication in Control-Hardware-in-the-Loop (CHIL) scenarios occurs over Ethernet, the IPM can be positioned to enable data tampering as required. In the test case considered, the IPM is positioned between the RTAC and relay to tamper with GOOSE messages sent by the RTAC, leading to incorrect settings and subsequent relay misoperation during faults. Additionally, the framework supports capabilities such as delaying, jittering, duplicating, and corrupting data packets.

Wireshark is employed to capture GOOSE packets which allows for effective monitoring and verification of the intrusion process.

4 | Implementation of the SGOC Protection Scheme Through the Developed Cyber-Physical Testbed

The basic adaptive protection scheme discussed in Section 2 is implemented in the cyber-physical testbed described in Section 3 to demonstrate the capability and utility. The 7-bus microgrid, depicted in Figure 1, with all the necessary protection features, is constructed using RSCADfx and executed in the RTDS NovaCor environment. For the HIL verification, three relays, namely, R5, R3, and R8, are selected. Specifically, SEL 421, SEL 751, and SEL 311C are used as replacements for R5, R3, and R8, respectively. The corresponding relay setting values for all operating modes, as shown in Table 3, are written into the time OC elements (51) of the relays' different SGs utilizing AcSElerator Quickset software.

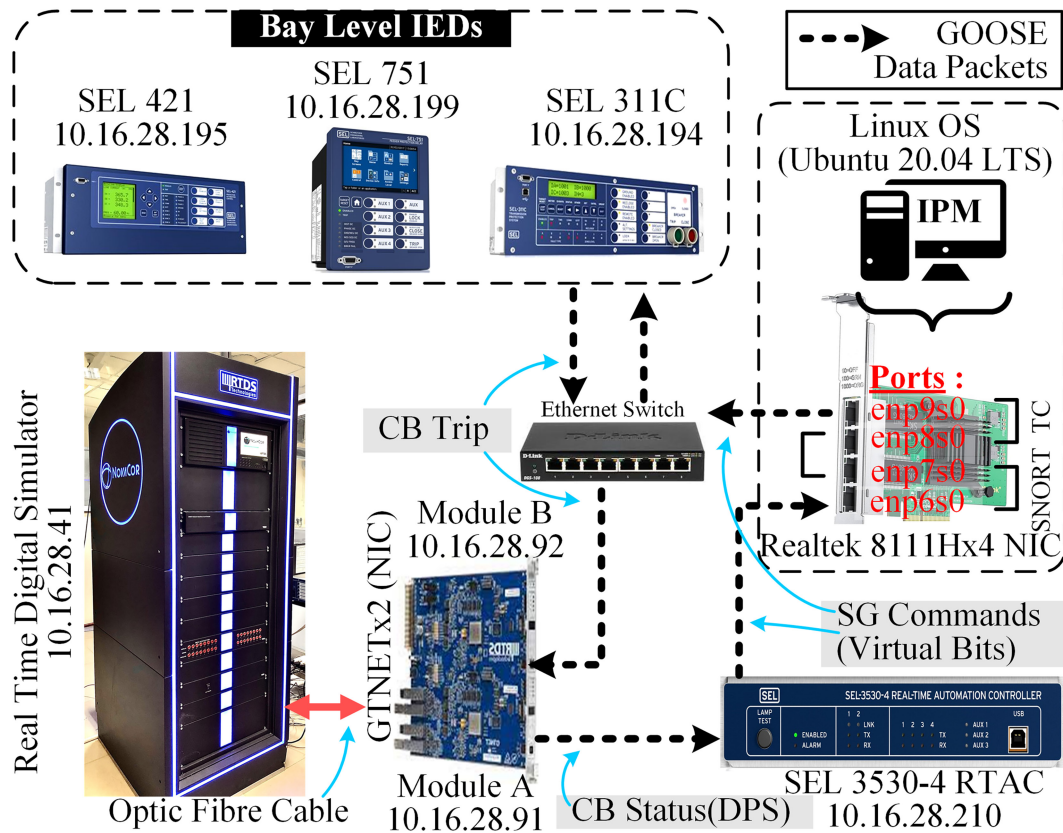


FIGURE 6 | Real-time data manipulation in live GOOSE streaming using IPM.

TABLE 6 | Switch statuses and corresponding operating modes, setting groups (SGs), and virtual bits.

Switch status			Operating mode	Setting group	Virtual Bits	
S1	SW1	SW2			VB002	VB001
1	1	1	GCM	SG1	0	0
0	1	1	IMM	SG2	0	1
1	0	0	GCR	SG3	1	0
0	0	0	IMR	SG4	1	1

As described in Section 3, the voltage and current signals for the hardware relays are provided through the GTA0 card. However, for SEL 421, high-level voltage and current signals are supplied using a voltage and current amplifier. During a fault event, the relay issues a trip command to the corresponding circuit breaker IEDs simulated in the RTDS system via the GOOSE protocol, thereby completing the protection loop.

The SG change algorithm, which relies on the status of switches S1, SW1, and SW2, is implemented in the SEL RTAC device. The SEL RTAC is interfaced with the RTDS system through GTNETx2. It receives the switch status signals from S1, SW1, and SW2, and based on Table 6 determines the appropriate SGs. The SG control command is transmitted to the relays using the GOOSE protocol, employing two virtual bits. The SEL RTAC software, AcSELeRator RTAC, is employed to manage the transmission and reception of data tags and to implement the algorithm.

4.1 | IEC 61850 GOOSE Configuration

In this paper, the IEC 61850 substation protocol has been utilized for communication within the protection system. IEC 61850 offers significant advantages over traditional substation communication protocols, thereby validating the practicality and sustainability of the proposed work. Its object-oriented data modeling enables more structured data representation compared to the flat structures of protocols like Modbus and DNP3 [45]. Additionally, IEC 61850 supports time-sensitive applications through GOOSE, ensuring high-speed and reliable communication for critical protection schemes that legacy protocols fail to meet [46, 47]. Unlike Modbus and DNP3, which often face interoperability challenges, IEC 61850 is designed for seamless integration across devices from different vendors, making it ideal for modern, multi-vendor substations [47, 48]. Furthermore, its scalability and flexibility make it well-suited for expanding systems, particularly in smart grids and renewable energy

applications, where older protocols require extensive modifications to meet growing demands. These features establish IEC 61850 as the preferred choice for advanced substation automation and justify its consideration in this paper.

The exchange of information, such as the switch status from the power network, SG change command from the microgrid controller, and trip command from the relays, is implemented using the GOOSE protocol. In this setup, the breaker IEDs, responsible for providing breaker status and opening the circuit breaker, are implemented in RSCAD. On the other hand, the external relays and microgrid controller serve as the hardware IEDs responsible for protection functions and control functions, respectively. Figure 7 illustrates the GOOSE configuration, showcasing both the external IEDs and the IEDs simulated in the RTDS simulator. The figure also depicts the GOOSE packet data attributes that carry the necessary data.

The configuration of IEDs for the GOOSE protocol is performed using dedicated configuration tools. In the case of the simulated IEDs in RTDS, an extension of RSCAD called the IED Configuration Tool (ICT) is utilized to configure the GOOSE settings. On the other hand, the external IEDs, including the relays and microgrid controllers, are configured using AcSElerator Architect, which serves as the GOOSE configuration tool

specifically designed for SEL devices. Table 7 provides the relevant information about the GOOSE signals, including the Logical Nodes (LNs), and data attributes employed in the testbed for the corresponding IEDs.

4.2 | Logical Architecture of the RIAD Mechanism

The underlying logic of the RIAD scheme is formulated and developed within the RTAC, utilizing industry-standard programming languages such as Continuous Function Chart (CFC) and Structured Text (ST), which adhere to the standards outlined in IEC 61131-3. Various classes, including AckVbs, CmVbs, and SwVbs, have been defined to serve distinct purposes, as shown in Figure 8. Additionally, global and local variables are declared to support these functionalities. In the figure, each block, referred to as a function block, represents an object instantiated from these classes to be employed in the logic. For each relay, an object is initialized from the AckVbs class, converting the corresponding SG into virtual bits (vb001/2_relay n). These bits are evaluated in real-time by a function block corresponding to the CmVbs class, displaying the current status of all connected relays, as depicted in Figure 8. As illustrated in Figure 8, the acknowledgment signal content (in the SPS.stVal datatype) is converted and compared with the actual local virtual bits corresponding

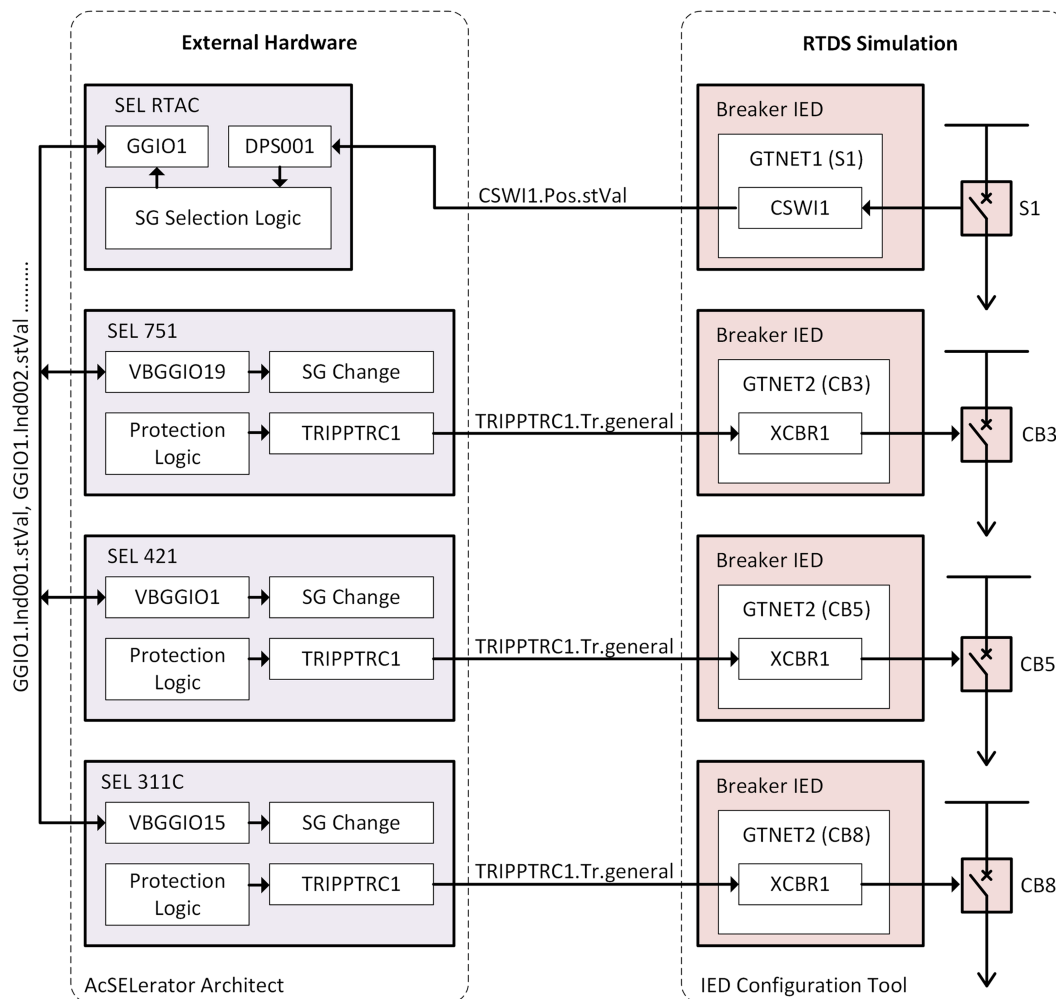
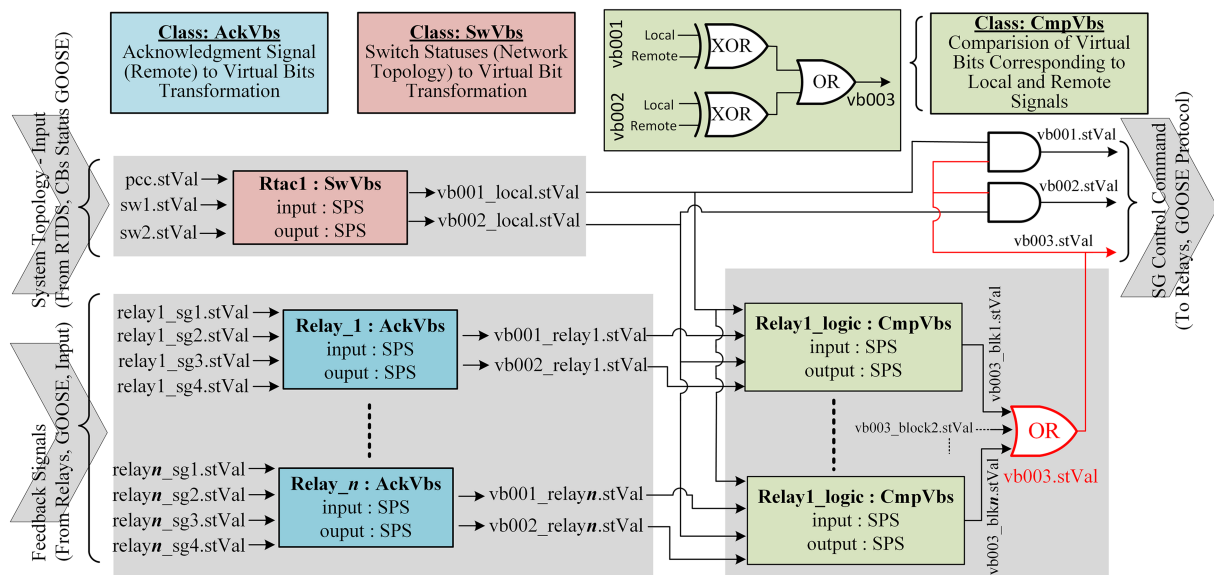


FIGURE 7 | Configuration of GOOSE messaging between IEDs.

TABLE 7 | GOOSE LNs and data attributes.

IED	LN	Data attribute	Function
S1	CSWI1	Pos.stVal	Switch status
SEL 751	TRIPTRC1	Tr.general	Trip signal
	GGION	Ind00n.stVal	SG status
SEL 421	TRIPTRC1	Tr.general	Trip signal
	GGION	Ind00n.stVal	SG status
SEL 311C	TRIPTRC1	Tr.general	Trip signal
	GGION	Ind00n.stVal	SG status
SEL RTAC	GGION	Ind00n.stVal	SG change, alert flag
	GGION	Ind00n.stVal	Retrieval of SG status

Note: n : integer

**FIGURE 8** | Operational flow of the RIAD mechanism in the microgrid controller.

to the circuit breaker status at the PCC and two other locations (SW1 and SW2) with the aid of SwVbs. Discrepancies between local and remote statuses trigger an RTAC-generated alarm (via vb003.stVal), alerting operators to potential misconfigurations or cyber-attacks impacting the communication of active virtual bits to the relays.

1. Mismatch in active SGs (remote) among the relays (mutual validation).
2. Mismatch between the local and remote relay word bits corresponding to active SGs (global validation).

Furthermore, the proposed scheme also informs the operators if there is a compromise in the health of the transmitted remote GOOSE message, indicating whether it is in a “good” or “invalid” state, thus ensuring the connectivity quality of the communication system.

5 | Results and Discussions

This section begins with a detailed explanation of the SG update mechanism, which is demonstrated in real-time. The subsequent analysis evaluates the performance of the protection system following the integration of this mechanism, with emphasis on primary and backup protection schemes using two distinct use cases. Each aspect is validated through real-time analysis, supported by comprehensive timeline presentations. The vulnerability of the conventional scheme to cyber-attacks is then examined, highlighting how such attacks can compromise the decision-making process of the centralized controller, leading to incorrect relay configurations and resulting protection system failures. To address these vulnerabilities, the proposed defense mechanism is first explained and demonstrated in real-time. It is then integrated with the protection system, and its effectiveness is validated through real-time analysis, successfully mitigating the risk of relay misoperation.

5.1 | Case 1: Changing Relay SG

A highly precise timeline, down to the nanosecond level, was constructed to analyze the use of RTAC to change the relay SGs after islanding (Figure 9). The moment of switch action was captured through the runtime of RSCAD, while the instance of SG change was recorded by adding the CHSG word bit from SEL 421 to the event recording bits list. These data were further analyzed using SynchroWAVE Event. Wireshark, a network protocol analyzer, was utilized to capture the timing of GOOSE (Generic Object-Oriented Substation Event) packet publishing from both RSCAD and RTAC, revealing the processing time taken by RTAC to send the SG change command to the relays.

Following the isolation of the system, which occurred precisely at 8.30575 s after a time delay of 8.25 ms for the circuit breaker to open, an additional 1.045 ms were consumed for communication processing during GOOSE publishing. Subsequently, 4.173 ms were taken by RTAC to execute the algorithm responsible for determining the appropriate SGs and transmitting the command to SEL 421, occurring at 8.494327 s. After a delay of one-cycle set in the relay, SEL 421 responded to the SG change

command and eventually, at 8.508916667 s, the relay's SG successfully transitioned from SG1 to SG2. Overall, 0.211916667 s were taken for the entire process of changing relay SGs after the switching instance.

5.2 | Case 2: Primary Protection

The successful operation of primary protection is depicted in Figure 10, accompanied by a precise timeline analysis. A three-phase fault is intentionally applied at the 50% distance on lines 3 and 4, and the response of SEL 421 relay, acting as R5, is carefully observed. Essential information, such as the fault instance, CB5 trip signal instance, and the exact fault clearance time, is obtained from RSCAD. Additionally, the analog-to-digital conversion, relay pickup time, and relay operating time are verified using the event recording feature of SEL 421 relay.

At 29.27894999 s, the fault occurrence is recorded and approximately 2.633344 ms are taken for the fault current to reflect in the numerical relay measurement after the analog-to-digital conversion. The relay operating time, measured as 0.337394943 s, falls within the predefined constraints of the minimum

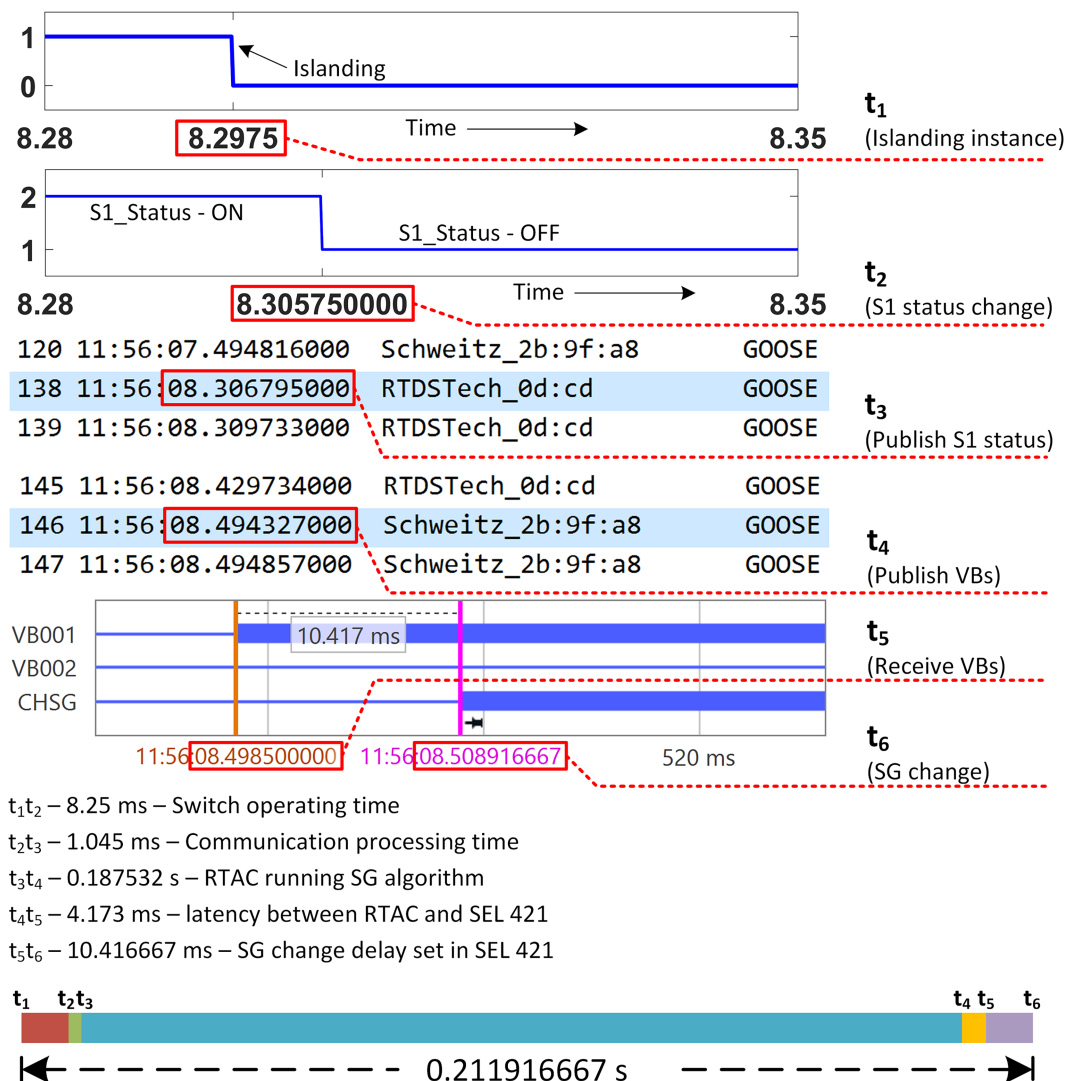


FIGURE 9 | Precise timeline analysis of relay setting group (SG) change.

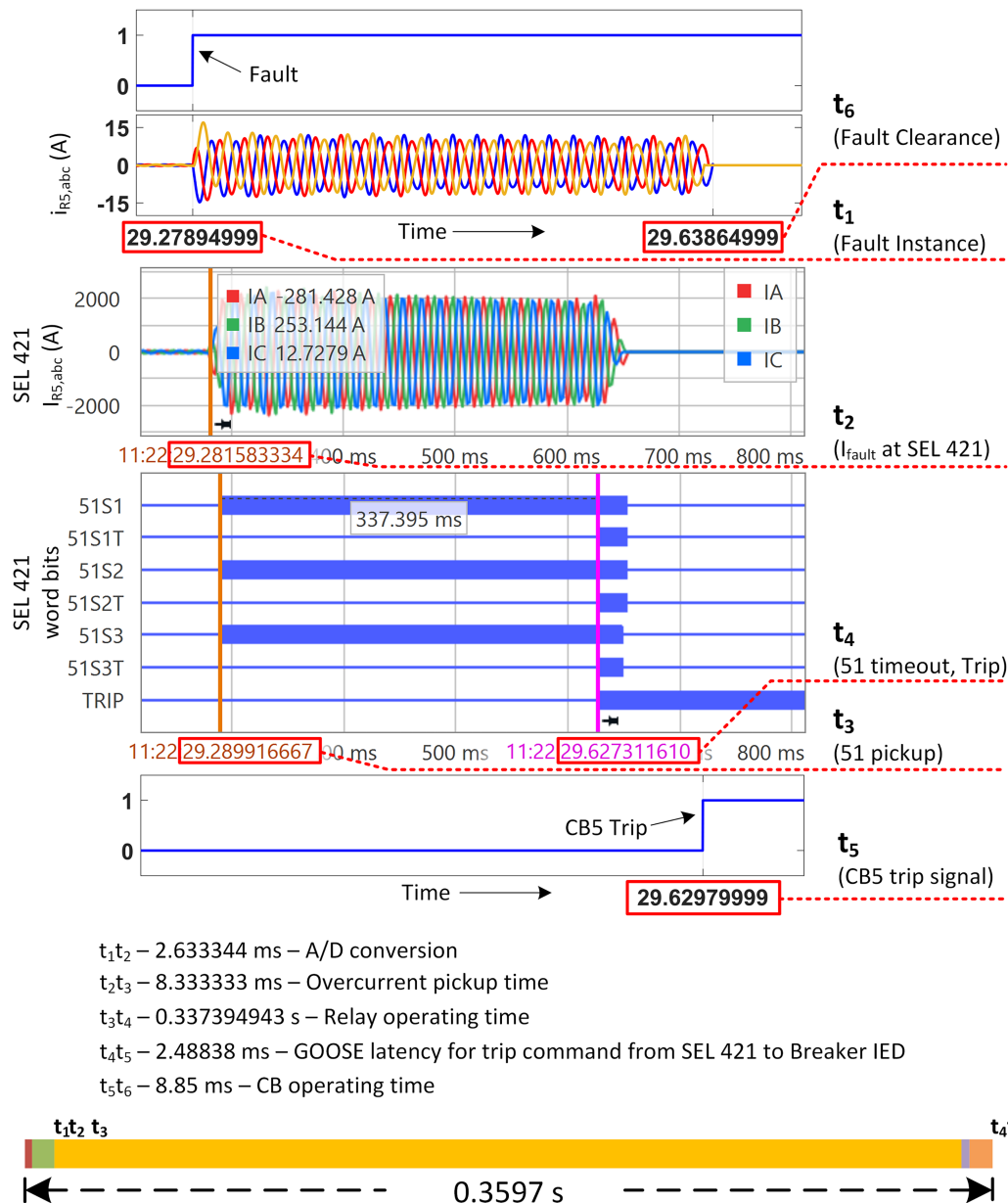


FIGURE 10 | verification of relay operating time in primary protection and timeline analysis.

and maximum operating time, as defined in [6] of Section 2. Furthermore, a latency of 2.48838 ms is observed in the GOOSE signal between SEL 421 and the CB controller IED modeled in RSCAD. It is observed that a total time of 0.3597 s is required to successfully isolate the faulty system after the fault occurrence.

5.3 | Case 3: Backup Protection

To verify the coordination between primary relay R5 and backup relay R3, a three-phase fault is deliberately applied at the midpoint of line 3-4. The operation of SEL 421 (primary relay) and SEL 751 (backup relay) is observed to assess their response. Furthermore, intentional CB malfunction is induced in CB5 to examine the operation of R3 as a backup relay. Similar to the previous case, fault instance, trip signals, and fault clearance

are observed through RSCAD plots, while the event recording feature in both numerical relays is utilized to analyze fault current pickup and timeout for the primary and backup relays. The coordination time interval is also recorded by analyzing event records from SEL 421 and SEL 751.

It is observed that despite SEL 421 picking up the fault current and issuing a TRIP signal with an operating time of 0.337378306 s, CB5 fails to operate, allowing the fault current to persist through the line (Figure 11). In parallel, SEL 751 as the backup relay also detects the fault current and issues a trip signal to CB3 at 60.152473004 s, successfully clearing the fault. The coordination time interval (CTI) is measured to be 0.968184031 s, which falls within the defined constraints of the coordination CTI as specified in [7]. Overall, it takes a total of 1.32885 s to clear the fault using the backup protection scheme.

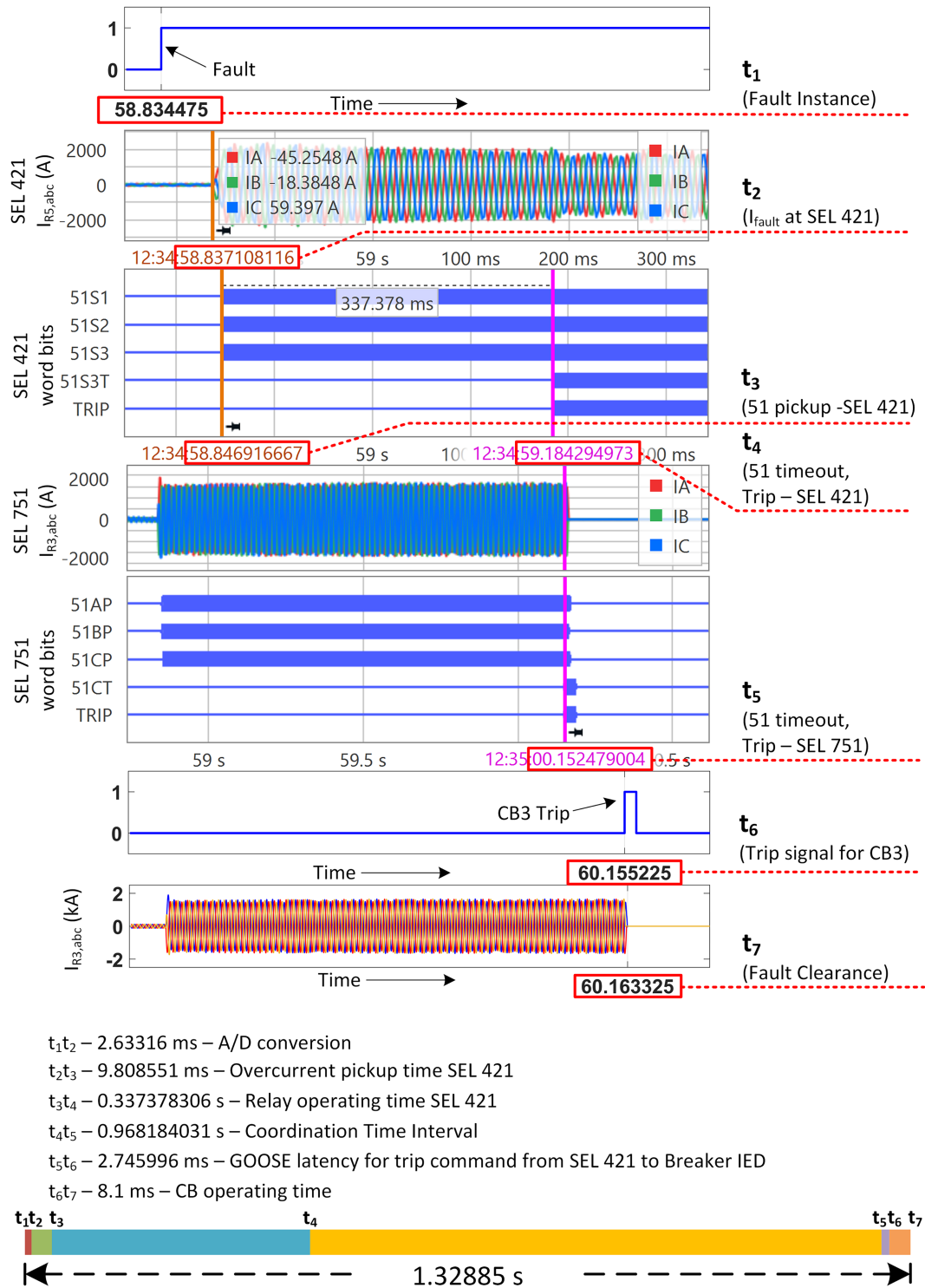


FIGURE 11 | Analysis of backup protection and relay coordination between relays R5 and R3.

5.4 | Case 4: FDI Attack on Control Commands (SG Word Bit) for the Relays

In centralized adaptive protection schemes, the presence of a reliable communication channel is crucial as it plays a vital role in transmitting critical SG control commands to the relays. However, in this study, the integrity of the communication link between the microgrid controller and the relays is compromised using the IPM described in Section 3.

The experiment is conducted in an islanded mode of operation, where the IPM injects a fabricated signal into the control command broadcasted by RTAC. False information is conveyed by this signal, misleading the relays to believe that the system is in a grid-connected mode (Figure 12a). As a consequence, an erroneous SG change command is issued within the relays by the attacker, utilizing virtual bits VB001 and VB002. Consequently, the relays adopt SG1, which is intended for grid-connected operation.

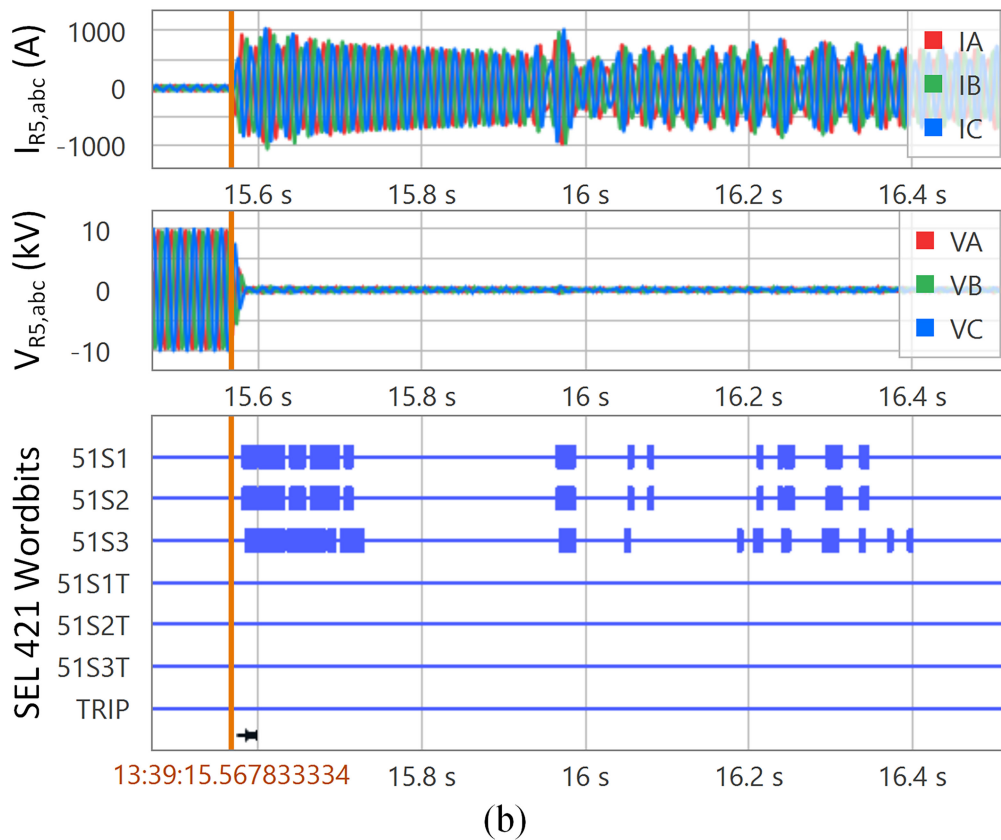
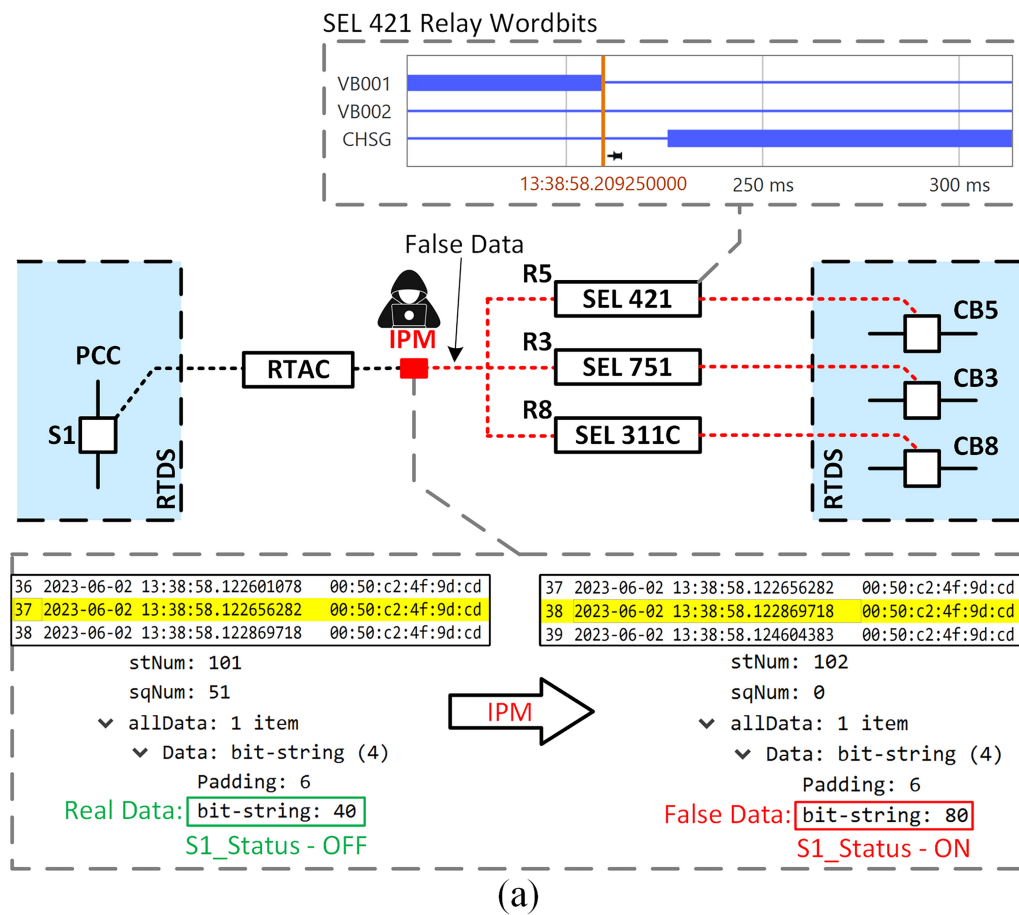


FIGURE 12 | FDI attack on PCC switch status signal. (a) Packet modification by IPM, consequent setting group change in the relay and (b) the maloperation of relay during fault.

The failure of relay operation during an actual fault scenario in this compromised situation is illustrated in Figure 12b. It is observed that due to a higher pickup current setting in the relay, the OC element fails to pick up and sustain. Consequently, it fails to generate the necessary trip signal to operate the circuit breaker.

5.5 | Case 5: Real-Time Validation of the RIAD Mechanism During Normal Operation

This section delineates the real-time operation of the proposed RIAD scheme, which operates in conjunction with the centralized SGAO protection scheme, in response to normal topological change in the system. Figure 13 illustrates the sequence of events in a temporal progression, systematically indexed from 1 to 10, which includes response of the proposed scheme implemented on RTAC to changes in both system topology and relays SGs, ensuring that all the relays are updated with the correct protection settings following a topological change. These events were recorded by RTDS during a routine transition in system topology specifically from a grid-connected mode to an islanding mode of operation. To monitor this chronology, an ICT tool within RSCAD is employed to configure the GOOSE data model, enabling the subscription to all pertinent statuses in the connected IEDs (Relays and RTAC) via GOOSE messages. Figure 14 illustrates a real-time validation of these events, as

depicted in Figure 13, using Wireshark. It includes screenshots from the Wireshark terminal, each corresponding to the individual captured events. These screenshots offer a visual representation with detailed annotations, including the same event indices (from 1 to 10), the corresponding timestamps of each event, and the associated GOOSE data packet information for each occurrence. The data packet information includes headers and payloads, which consist of datasets and their contents such as the GOOSE control block, among other elements. The depicted events are represented as binary statuses (i.e. 0 and 1). In both Figures 13 and 14, the transition in event index 1 (@ 22:49:15:469599) → 2 (@ 22:49:15:806677) signifies the change in the system topology, which is simulated in RTDS and depicted using status of the CB at PCC (0: open, islanded mode, and 1: closed, grid-connected mode). Upon detection by the RTAC, this transition prompts an alteration in the controlling virtual bits in RTAC, that is, the transition in event index 3 (@22:49:15:454567) → 4 (@ 22:49:15:941502), which is sent to the relays to change SGs. These virtual bits are instrumental in managing the SGs of the interconnected relays via the IEC 61850 GOOSE protocol. As previously mentioned, the activation of a block signal (event #5 @ 22:49:16:041625) denotes a discrepancy in the active SG among the connected relays. This signal persists until all relays are properly configured with the same SG (concluding with event #10 @22:49:19:441541). The events with indices transitioning from 8(@22:49:16:119096) → 9(@22:49:19:080032) and 6 (@22:49:17:737531) → 7(@22:49:18:034277) are indicative

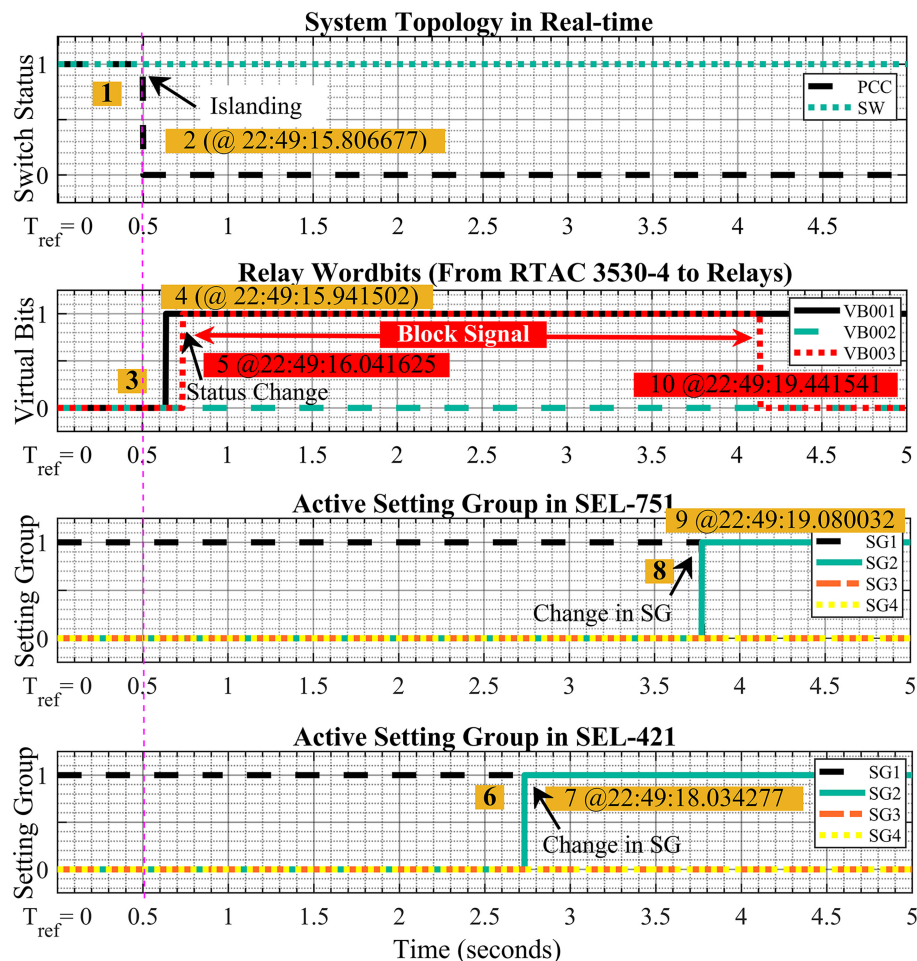


FIGURE 13 | Chronological sequence of operations.

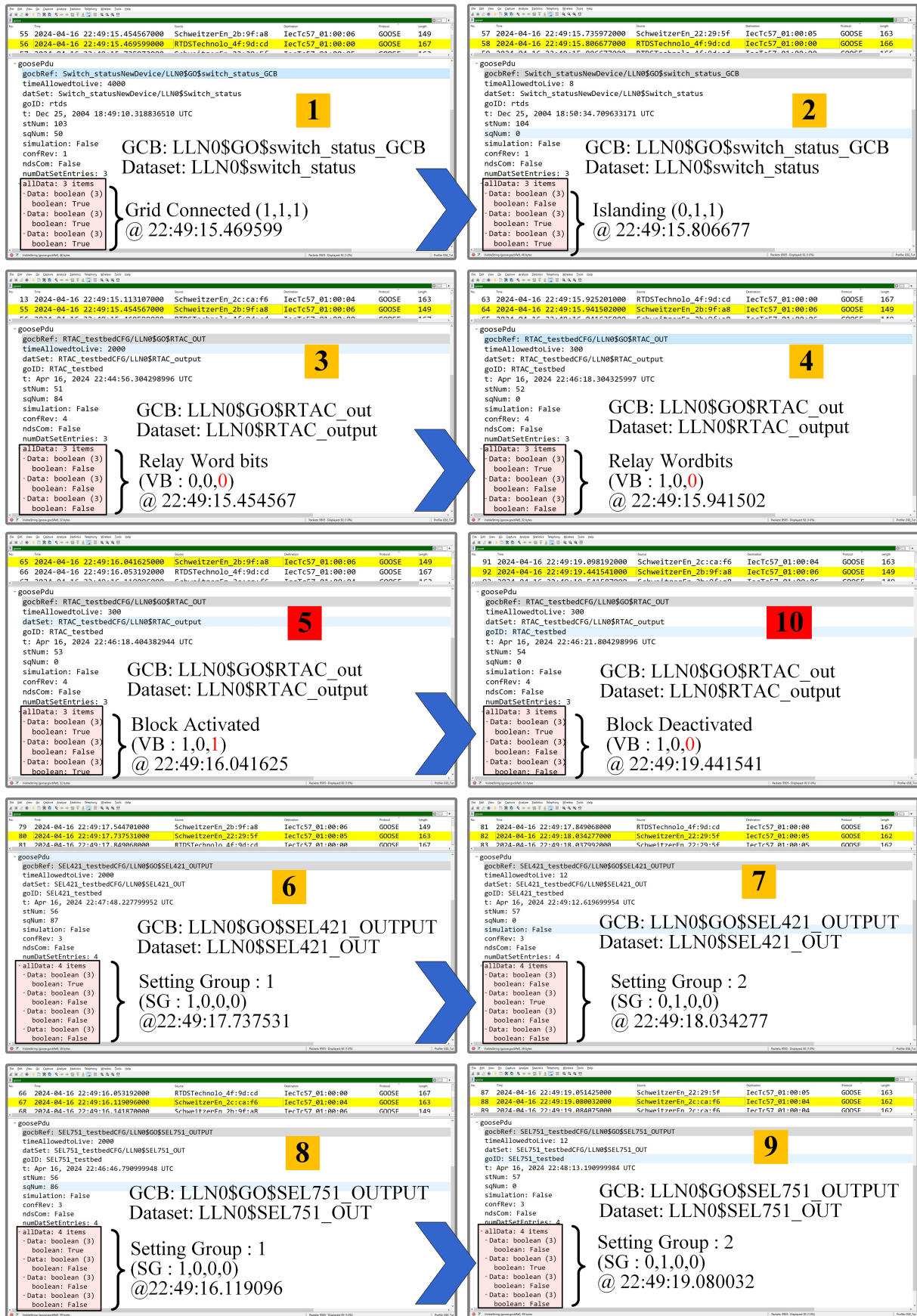


FIGURE 14 | Real-time operations validation with Wireshark.

of the SG changes in the SEL 421 and SEL 751 relay models, respectively, in response to the receipt of controlling VB issued by RTAC. The event corresponding to the transition 8 → 9 was recorded by the SEL 751 and subsequently analyzed using the SEL 5601-2 SynchroWAVE event tool for post-event assessment, as depicted in Figure 15.

5.6 | Case 6: Real-Time Response of the RIAD Mechanism to Attacks Targeting SG Control Commands

This section delineates the real-time operation of the proposed RIAD scheme in response to an FDIA attack targeting VB control commands sent by the RTAC, leading to the activation of incorrect SGs in the relays. As mentioned in section IV. B, the proposed scheme triggers a block signal when discrepancies arise either among the active SGs of the connected relays (or IEDs) or between the actual SG computed in the RTAC and the one active in the relays. This block signal ensures resilience against relay misoperation due to misconfigured relays, faulty relays, or relays affected by cyber anomalies—issues that cannot be diagnosed by the relays themselves. Figure 16 illustrates

real-time validation of this logic during a false data injection attack on the GOOSE message carrying an SG control command. The VB control command is broadcasted in the form of a GOOSE message from the RTAC to the relays. Figure 16 depicts a sequence of events indexed from 1 to 4. Event #1 (@19:55:28.045293) corresponds to the inception of the FDIA (False Data Injection Attack) in the communication channel. Subsequently, SEL 421 changes its SG in response to the attack (Event #2 @19:55:30.139303). Notably, the relays are unable to differentiate between the actual and manipulated signals. Event #3 (@19:55:30.444739) represents the block signal triggered by the RTAC, indicating an anomaly in the relay configuration. This signal persists until the issue is resolved. Finally, event #4 (@19:55:31.268027) corresponds to the change in the SG of SEL 751 in response to the FDIA attack. In the test case, the actual network topology is grid-connected, and the active SG should correspond to SG1. RTAC controls this SG through broadcasted control commands. However, the attacker intercepts and manipulates the virtual bits of the actual control signal from SG1 to SG2—an alteration that cannot be validated by the relays locally. The activation of the block signal alerts grid operators and prevents unprecedented failures, outages, and maintenance of the relays.

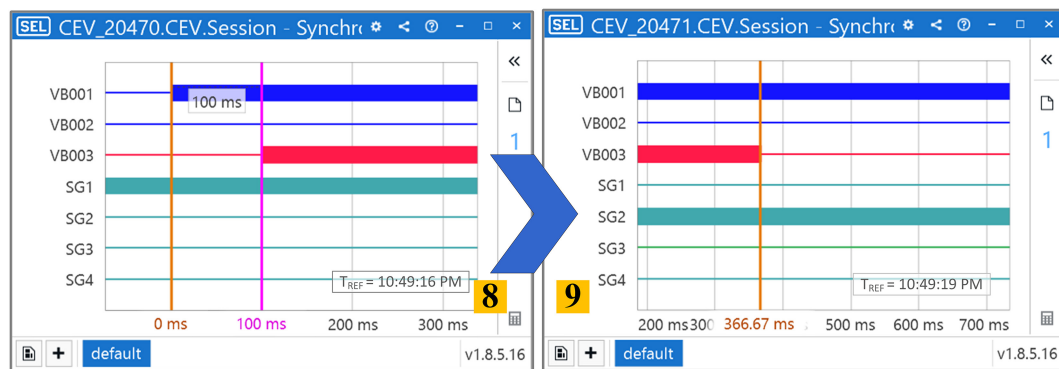


FIGURE 15 | Real-time Validation of SEL 751 operations with SEL SynchroWAVE Event Tool.

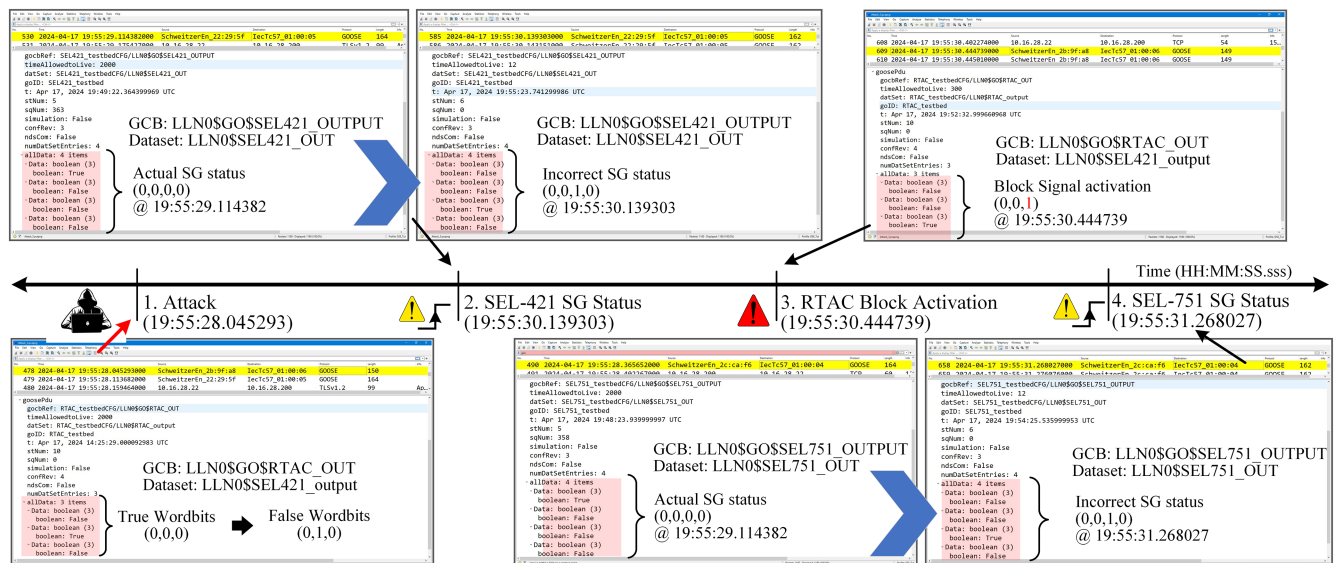


FIGURE 16 | Chronological account of SGAO responses to FDIA attacks.

6 | Conclusion

In this work, we present a comprehensive cyber-physical power system testbed designed for the simulation and analysis of SGAO protection in modern power systems. The testbed integrates the Relay Integrity and Attack Detection (RIAD) mechanism, which ensures the integrity of relay settings that may be vulnerable to misconfigurations from attacks over communication channels within the substation LAN, thus enhancing the overall reliability of the protection system. Traditional SGAO schemes often lack resilience to such misconfigurations resulting from cyber threats. Additionally, the testbed utilizes a Global Positioning System (GPS) based clock for precise synchronization of hardware and operations, which is crucial for the time-critical operation of protection systems during faults. Through extensive case studies, we demonstrate the testbed's effectiveness in replicating real-world scenarios and evaluating protection schemes under realistic conditions. By integrating communication system simulation with cyber intrusion analysis, the testbed provides a robust platform for assessing the impact of misconfigurations on protection systems. Overall, this developed testbed offers valuable insights and supports the development and implementation of effective benchmark protection schemes, advancing the field of cyber-physical power system protection.

Acknowledgments

The authors acknowledge the support from the Science and Engineering Research Board (SERB), Department of Science and Technology (DST), Government of India, under the scheme CRG/2020/005716, and the Central Power Research Institute (CPRI), Bangalore, Ministry of Power, Government of India (Grant No. : CPRI/R&D/TC/Trans/2022), to carry out this research work.

Data Availability Statement

The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

1. A. Ataee-Kachoei, H. Hashemi-Dezaki, and A. Ketabi, "Optimized Adaptive Protection Coordination of Microgrids by Dual-Setting Directional Overcurrent Relays Considering Different Topologies Based on Limited Independent Relays' Setting Groups," *Electric Power Systems Research* 214 (2023): 108879, <https://www.sciencedirect.com/science/article/pii/S0378779622009324>.
2. A. M. Entekhabi-Nooshabadi, H. Hashemi-Dezaki, and S. A. Taher, "Optimal Microgrid's Protection Coordination Considering n-1 Contingency and Optimum Relay Characteristics," *Applied Soft Computing* 98 (2021): 106741, <https://www.sciencedirect.com/science/article/pii/S1568494620306797>.
3. M. Ghalei Monfared Zanjani, K. Mazlumi, and I. Kamwa, "Application of μ PMUS for Adaptive Protection of Overcurrent Relays in Microgrids," *IET Generation, Transmission & Distribution* 12 (2018): 4061–4068, <https://digital-library.theiet.org/content/journals/10.1049/iet-gtd.2018.5898>.
4. H. Lin, K. Sun, Z.-H. Tan, et al., "Adaptive Protection Combined With Machine Learning for Microgrids," *IET Generation, Transmission & Distribution* 13, no. 6 (2019): 770–779, <https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/iet-gtd.2018.6230>.

5. M. N. Alam, "Adaptive Protection Coordination Scheme Using Numerical Directional Overcurrent Relays," *IEEE Transactions on Industrial Informatics* 15, no. 1 (2019): 64–73.
6. E. Purwar, D. N. Vishwakarma, and S. P. Singh, "A Novel Constraints Reduction-Based Optimal Relay Coordination Method Considering Variable Operational Status of Distribution System With DGS," *IEEE Transactions on Smart Grid* 10, no. 1 (2019): 889–898.
7. D. S. Kumar, D. Srinivasan, and T. Reindl, "A Fast and Scalable Protection Scheme for Distribution Networks With Distributed Generation," *IEEE Transactions on Power Delivery* 31, no. 1 (2016): 67–75.
8. M. Y. Shih, A. Conde, Z. Leonowicz, et al., "An Adaptive Overcurrent Coordination Scheme to Improve Relay Sensitivity and Overcome Drawbacks Due to Distributed Generation in Smart Grids," *IEEE Transactions on Industry Applications* 53, no. 6 (2017): 5217–5228.
9. M. Ghotbi-Maleki, R. M. Chabanloo, H. H. Zeineldin, et al., "Design of Setting Group-Based Overcurrent Protection Scheme for Active Distribution Networks Using MILP," *IEEE Transactions on Smart Grid* 12, no. 2 (2021): 1185–1193.
10. M. N. Alam, B. Das, and V. Pant, "Protection Coordination Scheme for Directional Overcurrent Relays Considering Change in Network Topology and OLTC Tap Position," *Electric Power Systems Research* 185 (2020): 106395, <https://www.sciencedirect.com/science/article/pii/S0378779620302017>.
11. P. Naveen and P. Jena, "Adaptive Protection Scheme for Microgrid With Multiple Point of Common Couplings," *IEEE Systems Journal* 15, no. 4 (2021): 5618–5629.
12. P. Naveen and P. Jena, "A Robust Protection Scheme for Multimicrogrids Using Fault Current Limiter," *IEEE Transactions on Industry Applications* 58, no. 5 (2022): 5763–5775.
13. V. A. Papaspiliotopoulos, G. N. Korres, V. A. Kleftakis, et al., "Hardware-in-the-Loop Design and Optimal Setting of Adaptive Protection Schemes for Distribution Systems With Distributed Generation," *IEEE Transactions on Power Delivery* 32, no. 1 (2017): 393–400.
14. J. Y. R. Wong, C. Tan, A. H. A. Bakar, et al., "Selectivity Problem in Adaptive Overcurrent Protection for Microgrid With Inverter-Based Distributed Generators (IBDG): Theoretical Investigation and HIL Verification," *IEEE Transactions on Power Delivery* 37, no. 4 (2022): 3313–3324.
15. A. K. Soni, A. Kumar, R. K. Panda, et al., "Adaptive Coordination of Relays in AC Microgrid Considering Operational and Topological Changes," *IEEE Systems Journal* 17, no. 2 (2023): 3071–3082.
16. M. P. Vinod, K. R. Satheesh, K. Madhusoodana, et al., "Numerical Relay Development Environment," in *2014 International Conference on Advances in Electrical Engineering (ICAEE)*, (2014): 1–4.
17. M. N. Uddin, N. Rezaei, and O. Emmanuel Olufemi, "Adaptive and Optimal Overcurrent Protection of Wind Farms With improved reliability," *IEEE Transactions on Industry Applications* 58, no. 3 (2022): 3342–3352.
18. F. Coffele, C. Booth, and A. Dyško, "An Adaptive Overcurrent Protection Scheme for Distribution Networks," *IEEE Transactions on Power Delivery* 30, no. 2 (2015): 561–568.
19. E. C. Piescorovsky and N. N. Schulz, "Fuse Relay Adaptive Overcurrent Protection Scheme for Microgrid With Distributed Generators," *IET Generation, Transmission & Distribution* 11, no. 2 (2017): 540–549, <https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/iet-gtd.2016.1144>.
20. Z. Yang, Y. Wang, L. Xing, et al., "Relay Protection Simulation and Testing of Online Setting Value Modification Based on RTDS," *IEEE Access* 8 (2020): 4693–4699.

21. A. A. Memon and K. Kauhaniemi, "Real-Time Hardware-in-the-Loop Testing of IEC 61850 Goose-Based Logically Selective Adaptive Protection of AC Microgrid," *IEEE Access* 9 (2021): 154612–154639.
22. T. Khurshaid, A. Wadood, S. Gholami Farkoush, et al., "Improved Firefly Algorithm for the Optimal Coordination of Directional Overcurrent Relays," *IEEE Access* 7 (2019): 78503–78514.
23. K. A. Saleh, H. H. Zeineldin, A. Al-Hinai, et al., "Optimal Coordination of Directional Overcurrent Relays Using a New Time–Current–Voltage Characteristic," *IEEE Transactions on Power Delivery* 30, no. 2 (2015): 537–544.
24. A. Ameli, A. Hooshyar, and E. F. El-Saadany, "Development of a Cyber-Resilient Line Current Differential Relay," *IEEE Transactions on Industrial Informatics* 15, no. 1 (2019): 305–318.
25. A. Ameli, A. Hooshyar, E. F. El-Saadany, et al., "An Intrusion Detection Method for Line Current Differential Relays," *IEEE Transactions on Information Forensics and Security* 15 (2020): 329–344.
26. A. Ameli, A. Ayad, E. F. El-Saadany, et al., "A Learning-Based Framework for Detecting Cyber-Attacks Against Line Current Differential Relays," *IEEE Transactions on Power Delivery* 36, no. 4 (2021): 2274–2286.
27. S. Chakrabarty and B. Sikdar, "Detection of Hidden Transformer Tap Change Command Attacks in Transmission Networks," *IEEE Transactions on Smart Grid* 11, no. 6 (2020): 5161–5173.
28. Y. M. Khaw, A. Abiri Jahromi, M. F. M. Arani, et al., "A Deep Learning-Based Cyberattack Detection System for Transmission Protective Relays," *IEEE Transactions on Smart Grid* 12, no. 3 (2021): 2554–2565.
29. A. Ahmed, V. V. G. Krishnan, S. A. Foroutan, et al., "Cyber Physical Security Analytics for Anomalies in Transmission Protection Systems," in *2018 IEEE Industry Applications Society Annual Meeting (IAS)*, (2018): 1–8.
30. J. Hong, R. F. Nuqui, A. Kondabathini, et al., "Cyber Attack Resilient Distance Protection and Circuit Breaker Control for Digital Substations," *IEEE Transactions on Industrial Informatics* 15, no. 7 (2019): 4332–4341.
31. P. Dubal, S. Das, and T. S. Sidhu, "Wide Area Measurement-Based Cyber-Attack-Resilient Breaker Failure Protection Scheme," *IEEE Transactions on Smart Grid* (2024): 1–1.
32. M. Silveira, "IEC 61850 Network Cybersecurity : Mitigating Goose Message Vulnerabilities," (2019), <https://api.semanticscholar.org/CorpusID:202637791>.
33. N. K. Kandasamy, "An Investigation on Feasibility and Security for Cyberattacks on Generator Synchronization Process," *IEEE Transactions on Industrial Informatics* 16, no. 9 (2020): 5825–5834.
34. O. Nzimakou and A. Rajapakse, "Real Time Simulation of a Microgrid With Multiple Distributed Energy Resources," in *2016 International Conference on Cogeneration, Small Power Plants and District Energy (ICUE)*, (2016): 1–6.
35. "IEEE Draft Guide for Protective Relay Applications to Transmission Lines," (2014), IEEE PC37.113/D7.0, August 2014, 1–0.
36. M. N. Alam, B. Das, and V. Pant, "Protection Coordination Scheme for Directional Overcurrent Relays Considering Change in Network Topology and OLTC Tap Position," *Electric Power Systems Research* 185 (2020): 106395, <https://www.sciencedirect.com/science/article/pii/S0378779620302017>.
37. J. M. Gers, E. J. Holmes, and I. of Electrical Engineers, *Protection of Electricity Distribution Networks*, IEE Power and Energy Series (Institution of Electrical Engineers, 1998), <https://books.google.co.in/books?id%3D0-ISAAAAMAAJ>.
38. B. R. Bhalja, R. P. Maheshwari, and N. Chothani, *Protection and Switchgear* (Oxford Higher Education, 2011).
39. H. F. Habib, N. Fawzy, M. M. Esfahani, et al., "An Enhancement of Protection Strategy for Distribution Network Using the Communication Protocols," *IEEE Transactions on Industry Applications* 56, no. 2 (2020): 1240–1249.
40. H. C. Kiliçkiran, B. Kekezoglu, and N. G. Paterakis, "Reinforcement Learning for Optimal Protection Coordination," in *2018 International Conference on Smart Energy Systems and Technologies (SEST)*, (2018): 1–6.
41. P. P. Bedekar and S. R. Bhide, "Optimum Coordination of Directional Overcurrent Relays Using the Hybrid GA-NLP Approach," *IEEE Transactions on Power Delivery* 26, no. 1 (2011): 109–119.
42. S. Biswal and S. R. Samantaray, "Relay Coordination Scheme in Microgrids Based on Non-Standard Tripping Curve of DOCRS With Multiple Setting Groups," *IEEE Transactions on Industrial Informatics* 20, no. 4 (2024): 5737–5749.
43. A. N. Sheta, B. E. Sedhom, A. Pal, et al., "Machine-Learning-Based Adaptive Settings of Directional Overcurrent Relays With Double-Inverse Characteristics for Stable Operation of Microgrids," *IEEE Transactions on Industrial Informatics* (2024): 1–10.
44. C. N. Devanarayana, "Chamara84," (2024), https://github.com/chamara84/snort-2.9_RTDS. Accessed: Sep., 2024.
45. A. Kostianinen and J. Valtari, "Applicability of IEC 61850 for Scada Communication With Centralized Protection and Control," in *Cired 2021 - the 26th International Conference and Exhibition on Electricity Distribution*, Vol. 2021, (2021): 1326–1330.
46. D. Njova, K. Ogudo, and P. Umenne, "Modelling the IEC 61850 and DNP3 Protocol Using OPNET in an Electrical Substation Communication Network," in *2022 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (ICABCD)*, (2022): 1–7.
47. D. D. Giustina, A. Dedè, G. Invernizzi, et al., "Smart Grid Automation Based on IEC 61850: An Experimental Characterization," *IEEE Transactions on Instrumentation and Measurement* 64, no. 8 (2015): 2055–2063.
48. D. Bojović, N. Obradović, and N. Kurjakov, "Improving Operational Efficiency and Reducing Costs in Distribution Utility With the Use of IEC 61850 Communication Protocol," in *2022 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-EUROPE)*, (2022): 1–5.

Appendix A

LINKNET Structure for Relay Coordination

The LINKNET structure is a specialized data structure used to efficiently store and manage network topology information in power systems, particularly in the context of relay coordination studies. This structure is especially beneficial in large-scale power networks, where manual scanning of network configurations would be impractical. By automating this process, LINKNET facilitates the identification of primary and backup relay pairs, ensuring that the relay coordination studies are both accurate and efficient, even in complex looped networks. The structure is composed of two algorithms: Algorithms I and II, as depicted in Figure A1.

Algorithm-I plays a crucial role in determining intermediate parameters by utilizing topological information essential for formulating relay coordination problems. The determination of backup relays for each primary relay is handled in Algorithm-II. The topological information is input to the Algorithms-I which are represented by specifying the connections between the nodes and the branches, assuming that the ends of each branch are indexed as shown in the equation below.

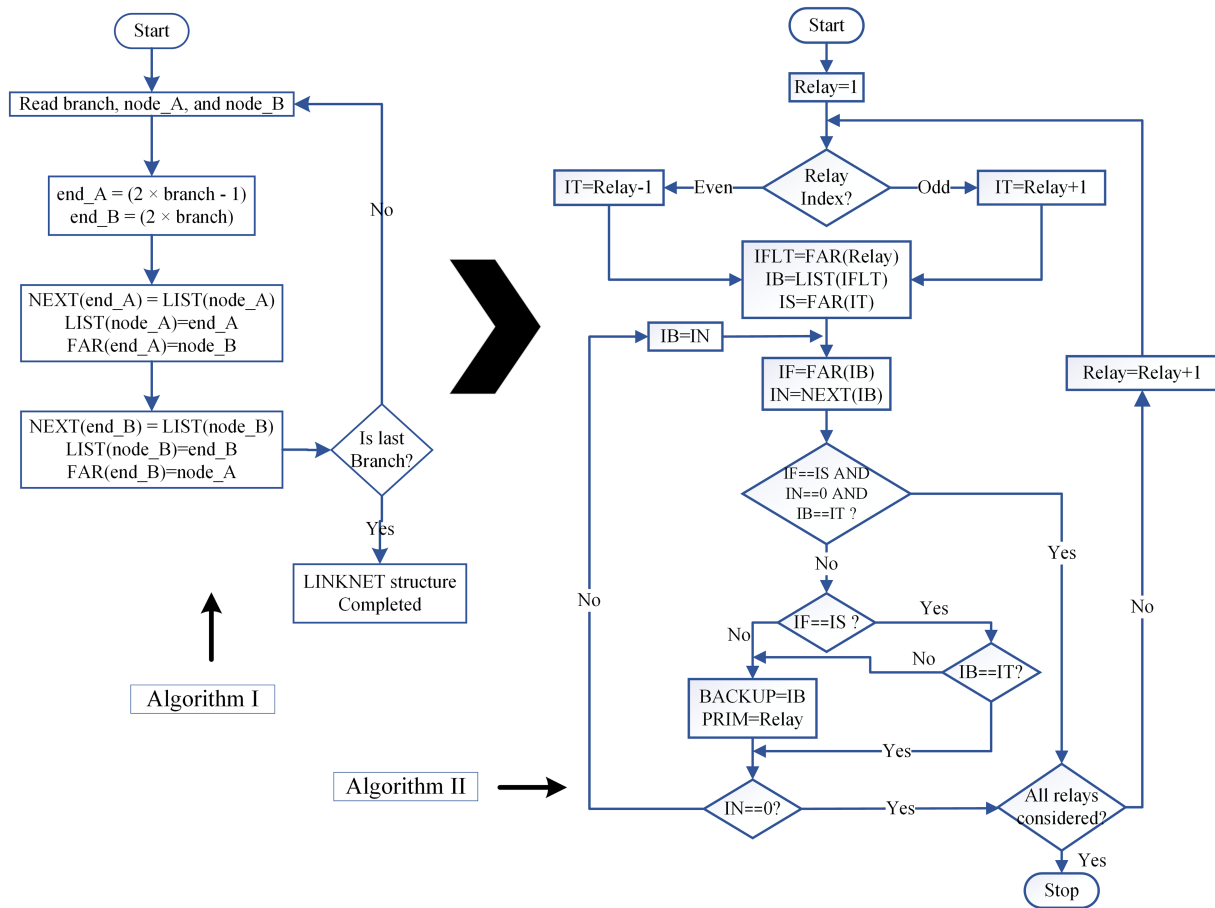


FIGURE A1 | LINKNET algorithm for relay coordination.

$$endA = f(branch) = (2 \times branch) - 1$$

$$endB = g(branch) = (2 \times branch)$$

Components of LINKNET, as computed in Algorithm-I, represent the network topology through three primary one-dimensional vectors:

1. **LIST Vector:** This vector is used to store all the bus links in the network. The dimension of the LIST vector corresponds to the number of buses in the system. Each entry in the LIST vector represents a bus and its associated links.
2. **NEXT Vector:** This vector stores the links between directional relays that are incident at a specific bus. The dimension of the NEXT vector is equal to the number of relays in the network. It helps in identifying connections between relays at a particular bus, which is critical for scanning the network during relay coordination studies.
3. **FAR Vector:** This vector is used to link any directional relay with its remote bus. The FAR vector also has a dimension equal to the number of relays in the system. It is instrumental in tracing relay connections to remote buses, which is essential for determining backup relay pairs.

Once these parameters are determined, Algorithm-II is used to compute primary and backup relays pairs, as depicted in Figure A1. Algorithm-II begins by considering one relay at a time and computing *IT*, with a condition based on whether its index is odd or even, as shown in Figure A1. Subsequently, other parameters such as *IFLT*, *IB*, *IN*, and *IS* are computed and further processed through various conditional

and assignment operations to determine the index of the backup relays corresponding to the primary relay under consideration. This process continues until all primary relays have been evaluated.