Energy Reports 12 (2024) 1655–1672

Contents lists available at ScienceDirect

Energy Reports

journal homepage: www.elsevier.com/locate/egyr

Research Paper

A hybrid physical and co-simulation modern adaptive power protection testbed for testing the resilience of smart grids under cyber-physical threats

Feras Alasali [a,*], Naser El-Naily [b], William Holderbaum [c,*], Haytham Y. Mustafa [b], Anas AlMajali [d,e], Awni Itradat [d]

[a] Department of Electrical Engineering, Faculty of Engineering, The Hashemite University, P.O. Box 330127, Zarqa 13133, Jordan
[b] College of Electrical and Electronics Technology-Benghazi, Libya
[c] School of Science, Engineering & Environment, University of Salford, Salford M5 4WT, UK
[d] Department of Computer Engineering, Faculty of Engineering, The Hashemite University, Zarqa 13133, Jordan
[e] Department of Computer Science and Engineering, American University of Sharjah, Sharjah 26666, UAE

ARTICLE INFO

Keywords:
Smart grid
Adaptive Protection
Cyber-attacks
Resilience
Renewable Energy

ABSTRACT

Power protection systems play a critical role in ensuring the safe and reliable operation of modern power grids. With the increasing complexity of grid topologies and the integration of Distributed Energy Resources (DERs), traditional protection schemes face challenges in maintaining effective coordination among relay systems. This paper presents a new adaptive Overcurrent Relay (OCR) protection and investigates the resilience of different traditional and new adaptive OCR protection schemes against various cyber-physical threats in a smart grid environment. Key contributions include the implementation of a novel adaptive protection scheme designed to dynamically adjust OCR settings based on real-time grid conditions, improving flexibility and responsiveness in managing grid variations induced by DER integration and operational changes. The proposed scheme is validated and implemented using the Multifunction Protection Relay SIEMENS 7SJ62, following to the programming standards of IEC 61131–3, ensuring the reliability and practical applicability of the adaptive OCR scheme in real-world scenarios. Additionally, a dedicated testbed is developed to simulate real-time cyber-physical interactions, incorporating hardware components such as the SIEMENS 7SJ62 and OMICRON-256 test device, along with high-performance computers and communication networks to facilitate comprehensive evaluations of adaptive OCR schemes under varying operational conditions. The study also examines the implications of real-time cyber-attacks on power system operations and the effectiveness of adaptive OCR protection schemes, addressing cybersecurity concerns and proposing mitigation strategies to the system resilience.

1. Introduction

1.1. Motivation and background

The smart grid plays a crucial role in development sustainable economic and societal networks. The current transformation of energy infrastructure includes generation, transmission, and distribution systems, emphasizing dependability and sustainability within the power network. Consequently, electric power systems have changed into intricately interconnected cyber-physical systems, heavily reliant on advanced communications. This reliance is caused by the integration of networked physical and electronic components, such as sensors, monitors, and control mechanisms, coupled to a central control center in the energy control and protection system (Habib et al., 2018a). However, the increased communication connection is leaving power systems more vulnerable to various cyber-attacks, potentially leading to unfavorable outcomes and cascade failures. The consequences can range from affecting networked essential infrastructure to endangering human lives. The basic goal of the power grid is the consistent delivery of electricity to certain load centers. The physical layer of large electric power networks is linked with a cyber system that includes information and communication technology. This comprises complex equipment and systems such as Supervisory Control and Data Acquisition (SCADA) systems and Intelligent Electronic Devices (IEDs), which are required for power systems' efficient and reliable operation (Hansen et al., 2017).

* Corresponding authors.
E-mail addresses: ferasasali@hu.edu.jo (F. Alasali), naseralnaile222@gmail.com (N. El-Naily), w.holderbaum@salford.ac.uk (W. Holderbaum), almahmoudy@ceet.edu.ly (H.Y. Mustafa), almajali@hu.edu.jo (A. AlMajali), itradat@hu.edu.jo (A. Itradat).

https://doi.org/10.1016/j.egyr.2024.07.051
Received 13 May 2024; Received in revised form 21 June 2024; Accepted 24 July 2024
Available online 1 August 2024

Nomenclature

DER	Distributed Energy Resource
OCR	Overcurrent Relay
SCADA	Supervisory Control and Data Acquisition
IEDs	Intelligent Electronic Devices
DN	Distributed Network
GOOSE	Generic Object Oriented Substation Event
SMV	Sampled measured value
MITM	Man-In-The-Middle
FDI	False Data Injection
IA	Integrity attack
RA	Replay Attack
DoS	Denial of Service
HIL	Hardware-in-the-loop
CPS	Cyber–physical system
CTI	Clearing Time Interval
CB	Circuit breaker
PV	Photovoltaic
TMS	Time Multiplier Setting
SW	Switching attack
CT	Current transformer
DI	Data integrity attack
CM	Current measurement
NT	Network topology
CFC	Continuous Function Chart

Table 1
Summary of adaptive OCRs coordination approaches for smart grids.

Ref.	Year	Protection Type	adaptive techniques	Hardware-in-the-loop	Verification in Industrial Relays	Cyberattack Threats
(Rahmati et al., 2015)	2014	OCR	Thevenin equivalent	×	×	×
(Papaspiliotopoulos et al., 2017)	2015	OCR	CB statuses	✓	×	×
(Alvarez de Sotomayor et al., 2018)	2017	OCR	CB statuses	×	×	×
(Núñez-Mata et al., 2018)	2018	OCR	CB statuses	×	×	×
(Ghalei Monfared Zanjani et al., 2018)	2018	OCR	Thevenin equivalent	×	×	×
(Alam, 2019)	2018	OCR	CB statuses	×	×	×
(Amin et al., 2020)	2019	OCR	CB statuses	×	×	✓
(Núñez-Mata et al., 2019)	2019	OCR	Energy Management Systems	×	×	×
(Alvarez de Sotomayor et al., 2018)	2020	OCR	CB statuses	✓	×	×
(Sampaio et al., 2020)	2020	OCR	multi-agent systems	✓	×	×
(Ataei and Gitizadeh, 2022)	2021	OCR	multi-agent systems	×	×	×
(Memon and Kauhaniemi 2021)	2021	OCR	CB statuses	✓	×	×
(El-Hamrawy 2022)	2022	OCR	CB statuses	×	×	×
(Dorosti et al., 2022)	2022	OCR	Fixed settings	×	×	×
(Yousefi kia et al., 2023)	2022	OCR	Fixed settings	×	×	✓
(Elrawy et al. 2023)	2023	OCR	CB statuses	×	×	✓
(Karimipour et al. 2023)	2023	OCR	CB statuses	×	×	✓
(Alasali et al., 2024a)	2023	OCR	CB statuses	✓	×	✓
(Abdelrahman et al. 2023)	2023	OCR	CB statuses	×	×	✓
(Gutierrez-Rojas et al., 2023)	2023	OCR	Energy Management Systems	×	×	×
(Ibtissam et al., 2022)	2023	OCR	CB statuses	×	×	×
(Alam et al., 2022)	2023	Recloser	multi-agent system	×	×	×
(Kasap et al. 2023)	2023	OCR	CB statuses	×	×	✓
(Bisheh et al., 2023)	2024	OCR	CB statuses	×	×	✓
(Pola et al., 2023)	2024	OCR	data-driven	×	×	×
(K. A and V. C 2024)	2024	OCR	data-driven	×	×	✓
(Mohamed et al. 2024)	2024	OCR	SVM	×	×	×
The proposed study		OCR	CB statuses and Currents value	✓	✓	✓

The use of these smart and modern systems and devices to manage circuit breakers, relays, transformers, capacitor banks, and other equipment causes power systems particularly vulnerable to cyber-attacks. As a result, managing the changing view of cyber threats is critical to ensuring the electrical grid's long-term stability and security.

The complex smart grid topology causes challenges for traditional protection schemes, leading to relay coordination failures. Overcoming these challenges is vital for robust protection schemes and the successful integration of smart topology into power systems. Resilience in power protection systems refers to the ability to withstand external disturbances while maintaining functionality. Effective coordination of protection relays is critical for the safe operation of smart power grid. Recent research focuses on adaptive protection schemes to address the impacts of DER integration within microgrids. These schemes utilize communication infrastructure within the Distributed Network (DN) to prevent coordination issues (Dennis Holstein and Cease, 2010; Habib et al., 2017a). However, reliance on communication links causes cyber-physical vulnerabilities, as modern digital relays lack internal validation checks. Therefore, this research investigates the resilience of traditional and adaptive OCR protection schemes against different cyber-physical threats in hybrid smart grid testbed, emphasizing the need for robust protection systems.

1.2. Literature review

To manage and control their operations, smart grids rely on advanced digital communication technologies. These technologies, however, can expose microgrids to cyber-physical risks, particularly in the form of False Data Injection (FDI) and Denial of Service (DoS) attacks, which are designed to manipulate the system's operation without detection. These attacks can cause significant disruptions by triggering unnecessary circuit breaker trips, leading to loss of power and potentially substantial economic impact (Hansen et al., 2017). A critical

aspect of smart grid security is distinguishing between electrical faults and malicious interference. Smart grids face unique challenges in fault detection compared to traditional power distribution systems. The non-linear relationship between fault current and fault distance, the bi-directional flow of power from DERs, and the differing responses between grid-connected and islanded modes all contribute to these challenges (Dennis Holstein and Cease, 2010; Habib et al., 2017a). Addressing these complexities is essential for ensuring microgrid stability and security in the face of evolving cyber threats.

In power protection systems, resilience refers to the system's ability to face external disturbances while maintaining or restoring functionality. Effective coordination of protection relays is crucial for the safe and cost-efficient operation of smart and microgrids, ensuring reliable relay operations during fault scenarios. Recent research, as described in Table 1, has concentrated on developing different adaptive protection schemes to address potential impacts of DER integration on radial and mesh power networks. These schemes utilize a communication infrastructure within the DN to prevent miss-coordination issues. However, modern digital relays based on traditional and adaptive protection schemes relying on communication links lack internal validation checks, making them vulnerable to distinguishing real faults or changing relay settings. Currently, there is a gap in research regarding the resilience of traditional and modern adaptive power protection systems against cyber-physical threats using real power distribution network specifications.

A key observation in many of the proposed adaptive protection schemes for microgrids is the reliance on robust communication structures. However, communication failures and cybersecurity threats pose significant risks to these systems, particularly when implementing fast, reliable adaptive protection mechanisms (Habib et al., 2018a). This characteristic vulnerability is a critical drawback in most adaptive protection designs. To address these problems, Habib et al. carried out a thorough assessment, focusing on the repercussions of communication failure in adaptive protection methods including energy storage devices (Habib et al., 2018a). In addition, they discovered in (Habib et al., 2018a; Hansen et al., 2017) that communication disruptions cause unverified relay settings, leaving adaptive protection solutions useless. The authors also investigated potential cyber-attacks, such as sending malicious code to overload relays or intercepting GOOSE communications to trigger circuit breakers. A real-world example of such cyber threats is the 2015 attack on the Ukrainian power grid by a Russian hacker group, as documented by Hansen et al. (2017). In this incident, hackers remotely manipulated substation breakers, causing a blackout that affected over 225,000 customers. This attack underscores the inherent vulnerabilities in IEDs and communication networks, particularly those based on IEC 61850 protocols, which are similar to other industry-distributed control systems using TCP/IP or Ethernet (Dennis Holstein and Cease, 2010). To mitigate these risks, various solutions have been proposed (Habib et al., 2017a, 2017b, 2018b), but challenges continue in achieving truly reliable adaptive protection schemes. While these proposals offer potential pathways to enhance the security and reliability of smart or microgrids, further research is needed to address these vulnerabilities effectively and ensure the resilience of adaptive protection systems in the face of communication failures and cyber threats.

Table 1 shows a significant lack of verification and cybersecurity focus among most adaptive OCR coordination approaches. Hardware-in-the-loop testing is a crucial step in validating the practical application of adaptive OCR schemes, where only a few studies included this form of testing. Similarly, industrial relay verification, which is vital for real-world validation, is rarely mentioned, raising concerns about the practical reliability of these approaches. Cybersecurity threats are a substantial risk to adaptive OCR coordination, with limited studies adequately address these issues. This review examines approaches to adaptive OCR coordination, focusing on the techniques used, verification through Hardware-in-the-loop (HIL) testing, industrial relay validation, and cybersecurity considerations. Table 1 provides a summary of these approaches, from 2014 to 2024, along with these key attributes. Early approaches to adaptive OCR coordination employed Thevenin equivalent methods (Rahmati et al., 2015; Ghalei Monfared Zanjani et al., 2018), offering theoretical insight but with limited practical application. Over time, circuit breaker (CB) status-based techniques became popular (Papaspiliotopoulos et al., 2017; Alvarez de Sotomayor et al., 2018; Núñez-Mata et al., 2018; Alam, 2019), providing a basic adaptive mechanism for relay coordination. Despite their adaptive nature, these methods often lacked severe verification and did not adequately address cybersecurity risks. Sampaio et al. (2020), Ataei and Gitizadeh (2022) introduced a broader range of techniques, including multi-agent systems, while Núñez-Mata et al. (2019), Gutierrez-Rojas et al. (2023) used energy management systems, and (Dorosti et al., 2022; Yousefi kia et al., 2023) employed fixed settings. These approaches represent a progression in adaptive OCR coordination, providing greater adaptability to evolving grid conditions. However, these studies failed to emphasize real-world testing or cybersecurity considerations, indicating gaps in reliability and security.

While Alam et al. (2022), Fu et al. (2015) introduced tools to identify cyber threats on power protection systems, their work did not specifically address the impact of cyber threats on different adaptive OCR configurations, with or without communication requirements. Effective adaptive OCR protection in microgrids must handle faults in both grid-connected and islanded modes, each with different fault current levels and paths. In (Mallouhi et al., 2011), OCR was tested and evaluated under cyber threats, but the evaluation was limited to the location closest to the fault. To address the interaction of cyber and physical factors, adaptive protection solutions must operate reliably and effectively. One potential approach is to connect all relays to a central administration system and send setting groups unidirectionally. However, this strategy is extremely costly in terms of capital and operating expenses and is based on conventional communication protocols (Gutierrez-Rojas et al., 2023). In previous studies (Gutierrez-Rojas et al., 2023; Adhikari et al., 2014), the authors evaluated the performance of adaptive OCR under DOS and FDI attacks in DN. However, their analysis did not include the influence of various cyber-attacks based on real hybrid smart grid testbed including OCR.

Testing emerging applications requires a realistic environment to characterize both physical and cyber components (Molina et al., 2013). Testbeds play a crucial role in understanding cyber-physical interactions and providing environments for prototyping novel applications. According to a survey on Cyber–physical system (CPS) education programs, 86 % of power system professionals acknowledge a global cybersecurity skill gap, and 92 % of power system recruiters encounter challenges in finding skilled candidates for CPS (Fu et al., 2015). In (National SCADA Testbed Program), the analysis of cyber-attacks on power systems is conducted using a comprehensive testbed that combines a simulated power grid with an emulated communication network. Real-world cyber events are simulated to validate security and performance. Similarly, (McDonald et al.) employs a cyber–physical testbed integrating industrial-grade SCADA software with a real-time digital simulator for non-real-time analysis. In (Mallouhi et al., 2011), a CPS testbed extends the large-scale testbed to simulate replay attacks, incorporating layers for power system dynamics, network measurement, software-defined networks, and application functionalities. Another study (Adhikari et al., 2012) introduces a testbed utilizing real-time power system simulators and fiber/ethernet networks to test smart and distributed management control. To investigate the effectiveness of stability control equipment under cyber events, including False Data Injection attacks (FDI) and Man-In-The-Middle (MITM) attacks, (Adhikari et al., 2014) presents a flexible HIL testbed. In (Adhikari et al., 2014), various power grid scenarios are considered, including the protection system for DN under different cyber-attacks by using OPAL RT simulator. Also, in another study (Adhikari et al., 2014), OPAL RT simulator testbed with SEL 351 S protection system is used to investigate

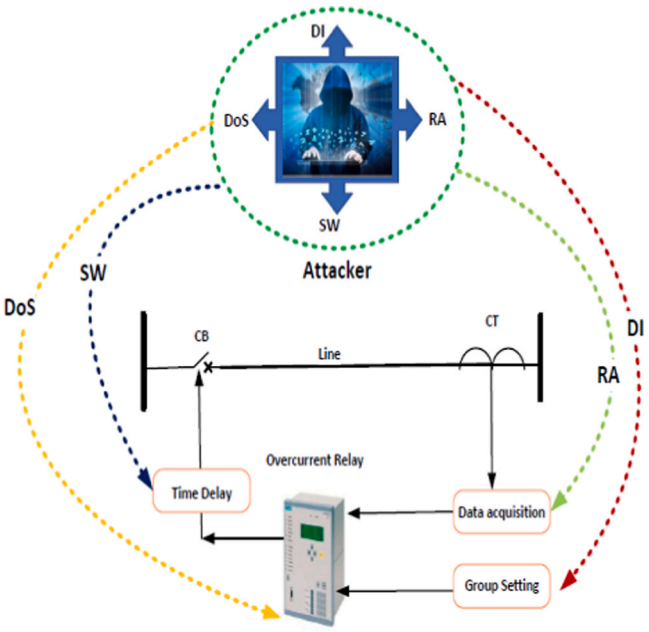


Fig. 1. Adaptive OCR schemes and potential cyber-physical threats.

Table 2
The group settings for the adaptive OCRs.

Group settings	Utility power source	PV power source
A	✓	×
B	✓	✓

Table 3
The group settings for the adaptive OCRs.

Group settings	Utility power source (CB)	PV power source (CB)	PV current contribution into the grid
A	✓	×	×
B	✓	✓	✓
C	×	✓	✓
D	This group setting will be activated during N - 1 contingencies, which include single outages such as line, substation, or DG failures, alongside smart grid operational modes.		

power grid security and performance under cyber-attacks based on load fluctuations and disabling two transmission lines. However, these studies did not investigate and test the impact of cyber-attacks on physical OCRs and adaptive protection schemes. The complicated interaction of cyber and physical components in these systems makes it difficult to be developed and tested, and there is limited research on evaluating traditional and adaptive OCR performance in the face of different cyber-physical threats. To address this gap, this paper presents and evaluates new adaptive protection schemes for OCR and current works that do not test on real smart hybrid protection testbed.

The resilience of the proposed method compared to existing approaches can be analyzed by examining key features and evaluations from previous studies. Traditional methods, such as those described in (Gutierrez-Rojas et al., 2023), often rely on centralized administration systems and unidirectional setting groups, which are costly and based on conventional communication protocols. These methods generally lack robustness against modern cyber threats. In contrast, the proposed method integrates adaptive techniques that consider both CB statuses and current values. This approach has been validated through HIL and simulations and tested in industrial relay settings, providing a comprehensive evaluation under realistic conditions. This methodological advancement enhances the accuracy and responsiveness of the protection mechanism, making it more resilient to various cyber-physical threats. Reviewing existing literature, as summarized in Table 1, traditional approaches predominantly focus on static CB statuses without adaptive capabilities or validation in industrial environments. For example, studies (Rahmati et al., 2015; Alvarez de Sotomayor et al., 2018), and (Núñez-Mata et al., 2018) primarily utilize Thevenin equivalents or CB statuses without adaptive features or thorough validation in industrial settings, limiting their ability to withstand dynamic cyber-physical threats effectively. The proposed method innovates by incorporating adaptive OCR techniques that dynamically adjust based on real-time CB statuses and current values. By applying HIL with simulations and validation in industrial relay settings, the proposed method ensures that resilience is not only theorized but substantiated through practical implementation. This approach fills a critical gap in existing research by offering a comprehensive solution that integrates adaptive techniques with real-world validation, thereby advancing the resilience of OCR systems in contemporary smart grid environments.

1.3. Contributions

In general, previous studies, as discussed in Section 1.2, have not examined or tested the effects of cyber-attacks on physical OCRs and adaptive protection schemes. The complex interaction between cyber and physical components in these systems presents challenges in their development and testing, with limited research available on evaluating the performance of traditional and adaptive OCRs against various cyber-physical threats. To fill this gap, this paper introduces and assesses adaptive and traditional protection schemes for OCRs, emphasizing the absence of testing on a real smart hybrid protection testbed in current works. The key contributions of this work are:

- Implementation of a novel protection scheme based on real-time adaptive protection method to be for more efficient under the proposed cyber-physical threats. The combination of CB statuses and current values provides a more adaptable and flexible solution for OCR coordination. This adaptability allows the proposed model to better meet the demands of smart grids, where load conditions and grid configurations can change frequently.
- Verification and applied the proposed novel scheme in real industrial relay (Multifunction Protection Relay SIEMENS 7SJ62) by utilizing an established format based on the IEC 61131–3 programming standard.
- Development of a real-time cyber-physical system testbed utilizing Multifunction Protection Relay SIEMENS 7SJ62, OMICRON-256 test device, high-performance computers, and communication networks. The testbed's capabilities are investigated in terms of power system protection and control. This comprehensive approach ensures that the adaptive OCR scheme is tested in conditions that simulate real-world scenarios, providing greater confidence in its reliability.
- Investigation of the impact of different real-time cyber-attacks on a protection power system, modern adaptive OCR protection schemes and power system operations. By focusing on cybersecurity, this model reduces vulnerabilities in adaptive OCR coordination, which is an area where many existing approaches fall short.

1.4. Outline of the paper

The subsequent sections of this paper are structured as follows: Section 2 describes the adaptive OCR schemes. Section 3 explains the cyber-physical threats to adaptive protection schemes. Section 4 presents the Cyber-physical power protection system testbed. Section 5 introduces the resilience evaluation of adaptive protection systems. Finally, Section 6 summarizes the key results of this study.

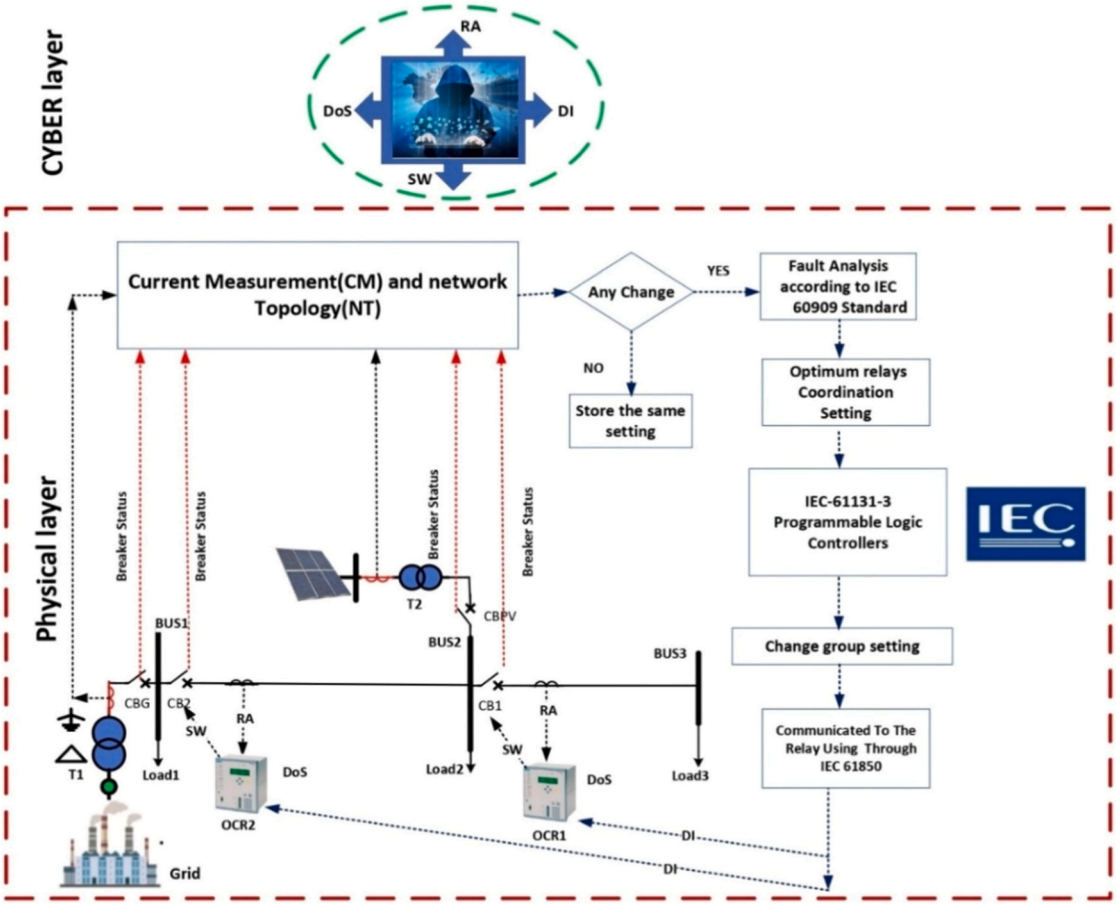


Fig. 2. Proposed adaptive OCR schemes.

2. Adaptive OCR schemes

2.1. Traditional recent adaptive OCR scheme

Adaptive protection systems are designed to enhance the flexibility and responsiveness of power system protection by allowing for real-time adjustments in response to changing network conditions. This study develops and evaluates modern adaptive protection system, as outlined in (Poudel et al., 2017; Alasali et al., 2024b; Shih et al., 2017). Fig. 1 illustrates a common approach in adaptive OCR scheme and potential cyber-physical threats, where the relay settings are adjusted based on the network's circuit breaker configuration, which indicates whether the system is operating in a traditional mode (with utility sources) or a grid-connected mode (integrating photovoltaic (PV) systems).

The initial step involves gathering data on circuit breaker status and other grid parameters to determine the current network topology, whether it is in grid-connected mode or islanding mode. Next, this information is compared to the previous state of the network topology. If the topology has not changed, the previously stored settings for the adaptive OCR are reused. However, if there is a significant change in the network topology, a combination of fault analysis and grid data need to be used to reconfigure the OCR settings to align with the new topology. This reconfiguration process involves solving an optimization problem, as described in Eqs. (1) and (2) (Hansen et al., 2017; Dennis Holstein and Cease, 2010), to identify the optimal configuration for the OCRs.

$$T_{tripping} = \min \sum_{r=1}^{R} \sum_{l=1}^{L} (t_{fl}) \tag{1}$$

$$T_r = \left[\frac{a}{\left(\frac{I_f}{I_p}\right)^b - 1} \mathrm{TMS} \right] \tag{2}$$

The objective function presented in Eq. (1) is designed to account for various factors, including selectivity constraints and the Clearing Time Interval (CTI), which measures the time difference between the tripping of primary and backup relays. This formulation ensures that OCR coordination provides effective protection while minimizing the risk of unnecessary tripping. Variables R and L represent the number of OCRs) and the fault location, respectively. The variable T_r represents the tripping time of the (r) OCR when a fault occurs at the (l) location. This approach to OCR coordination aims to ensure that the relays work in harmony, with primary relays operating before backup relays to prevent system-wide disruptions. OCRs typically operate with an inverse-time characteristic, where the tripping time decreases as the fault current increases. This relationship is mathematically described in Eq. (2), where T_r is the operating time of each OCR, I_f denotes the fault current, and I_p represents the relay's pickup current. The coefficients a and b, derived from the relay's characteristic curve, define the steepness and offset of the inverse-time relationship. These coefficients are crucial for calculating the Time Multiplier Setting (TMS), which adjusts the OCR's sensitivity to fault currents. In this research, the optimal TMS is determined to minimize tripping time while maintaining selectivity and the appropriate CTI between primary and backup relays. This optimization ensures that the protection system responds swiftly to faults without compromising overall system stability. The proposed approach leverages the Water Cycle Algorithm, allowing for a flexible and efficient method to find the ideal TMS, contributing to enhanced OCR

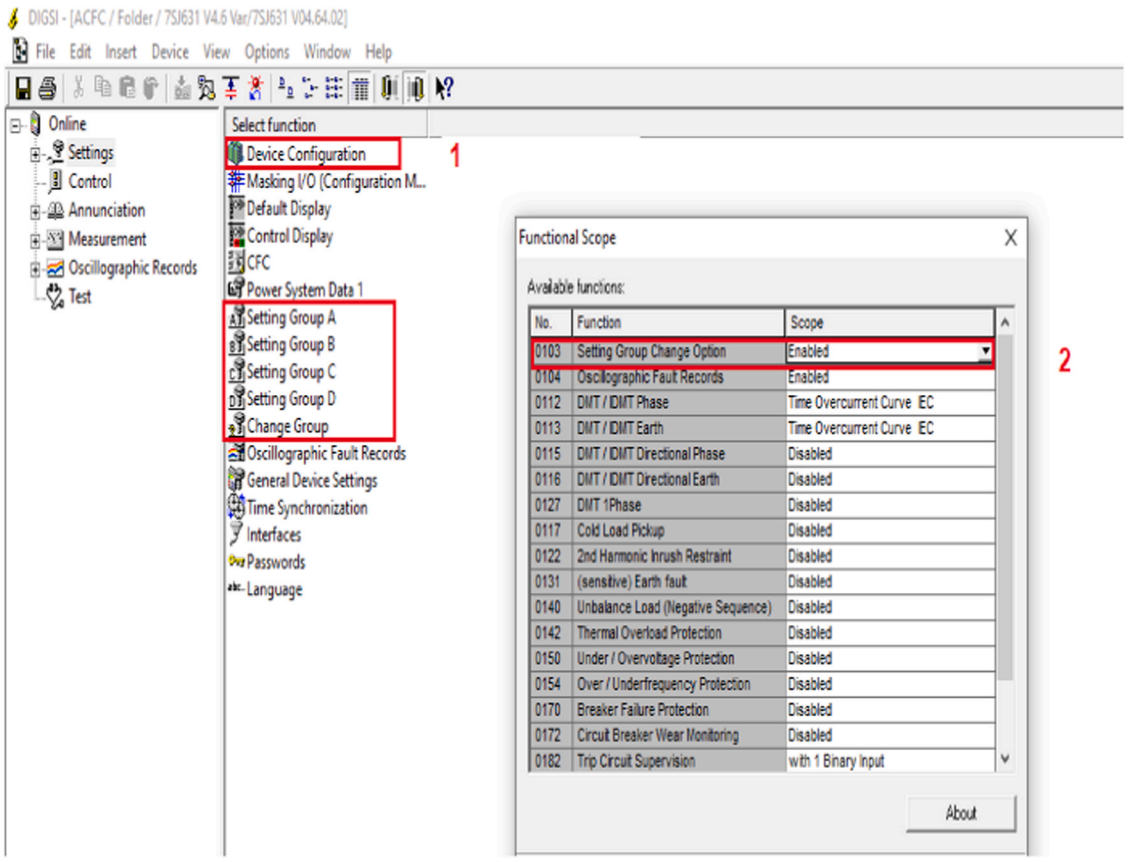


Fig. 3. Visualization of Data and Parameters Allocation in CFC Programming.

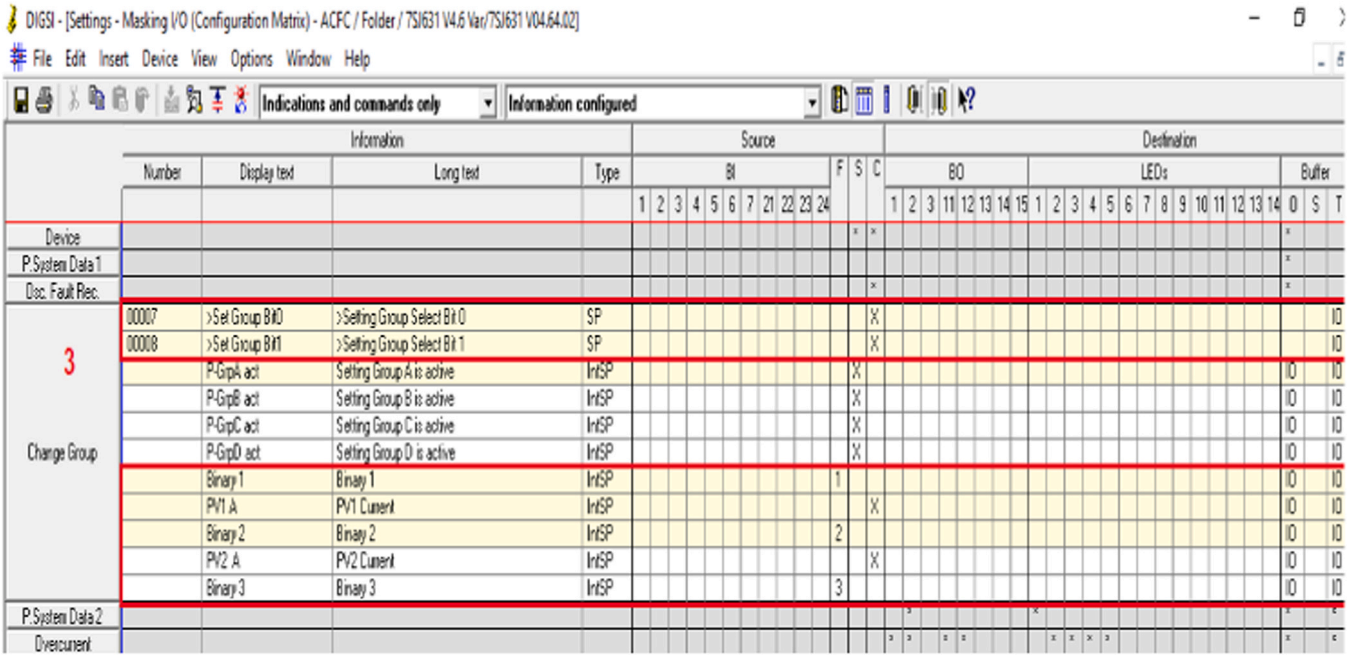
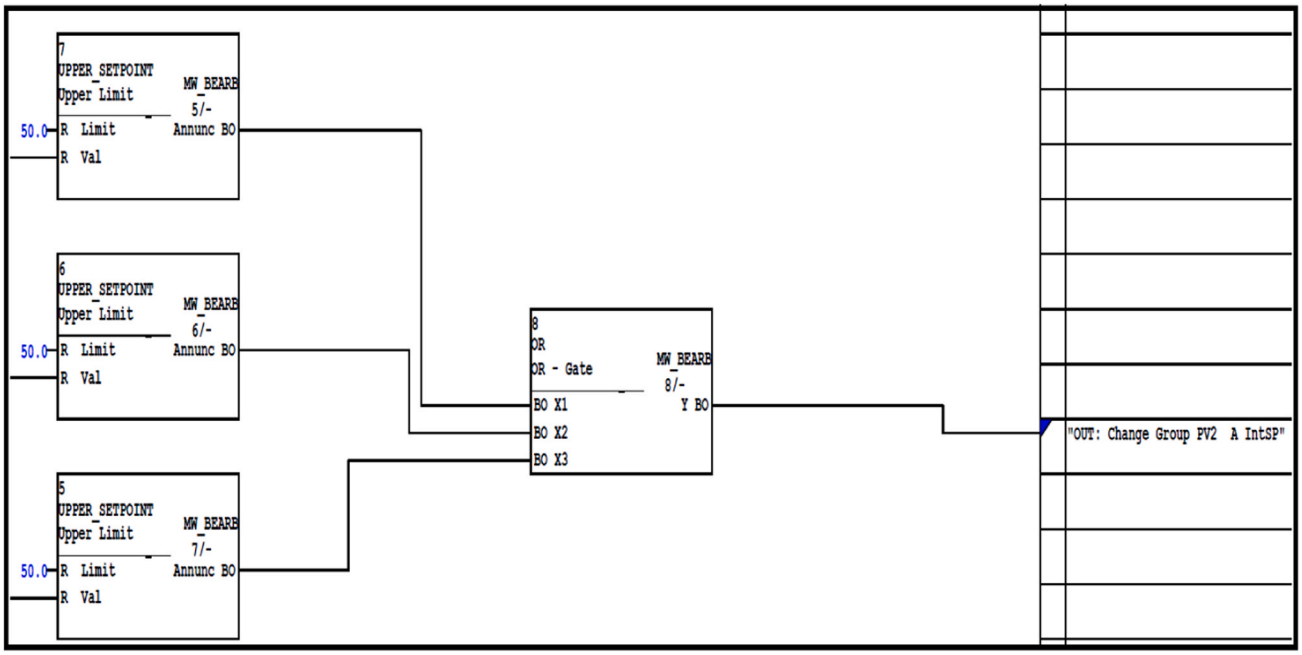


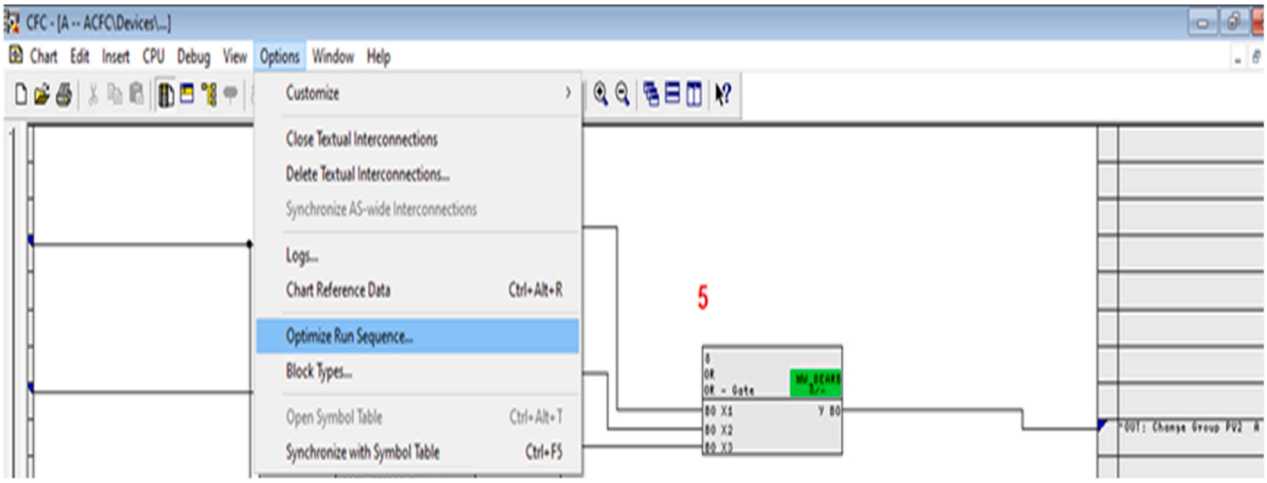
Fig. 4. Design of CFC Chart for Adaptive OCR Scheme Logic.

coordination and improved power system protection.

The Water Cycle Algorithm, a robust optimization technique inspired by the natural flow of water, is utilized to optimize the settings for OCRs. This algorithm is particularly effective for solving complex OCR coordination problems and is detailed in (El-Naily et al., 2022). The Water Cycle Algorithm finds the optimal OCR settings by simulating how water flows through rivers and converges at a common point, akin to how optimization works by converging on the best solution. After determining the optimal settings with the Water Cycle Algorithm, these configurations are applied through communication links to update the



(a)



(b)

Fig. 5. Validation of Run Sequence for CFC Chart in Adaptive OCR Scheme.

OCR settings. This research employs two distinct group settings for OCRs, as shown in Table 2, to ensure high sensitivity and selectivity in fault detection and relay coordination. The proposed adaptive OCR approach involves continuous monitoring of electrical parameters, with real-time communication being a critical component for transmitting OCR signals.

The implementation of this adaptive approach depends on OCRs' capability to automatically adjust their settings in real-time. This functionality allows the protection system to quickly adapt to changing grid conditions, enhancing the reliability and efficiency of OCR coordination. By leveraging the Water Cycle Algorithm's optimization capabilities, the proposed approach can identify the optimal relay settings, leading to more effective and responsive OCR coordination in dynamic power system environments.

2.2. *Proposed new adaptive OCR scheme*

The adaptive approach allows the protection system to respond to dynamic conditions within the power system, providing a more robust and flexible protection mechanism. By adjusting the OCR settings based on the network's operational mode and other critical parameters, the adaptive system can improve protection reliability and reduce the risk of false tripping or miscoordination. The research presented in this study contributes to the ongoing development of adaptive protection systems by offering insights into their operation and demonstrating their potential for enhancing power system protection in an evolving energy landscape.

Reports from the North American Electric Reliability Corporation (NERC)'s Protection System Misoperation Task Force indicate that over 20 % of protection system misoperations stem from relay and CB malfunctions (Alasali et al., 2024b). A significant contributor to these

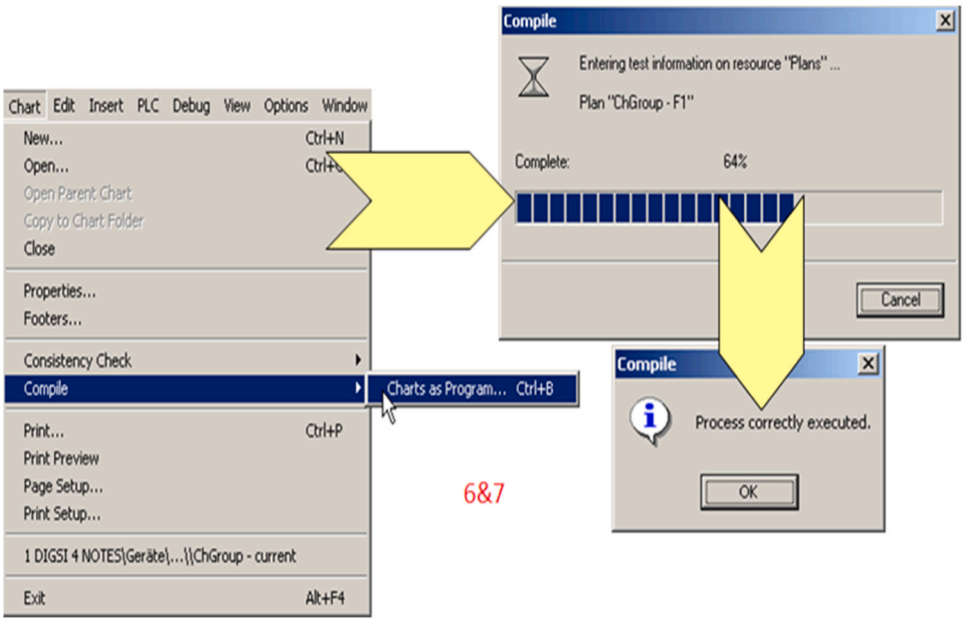


Fig. 6. Compilation Process of CFC Chart for Adaptive OCR Scheme.

Table 4
Proposed Novel Adaptive OCR Scheme Programming Steps with DIGSI CFC.

Step	Description
1	Allocate Necessary Information to CFC: all relevant data and parameters required for the CFC programming. This includes information about the network topology, fault scenarios, and relay settings. Ensure that all necessary inputs and outputs are identified and documented, as shown in Fig. 3. In addition, the setting group change option is enabled to allow the possibility of build and verify group setting approach, as shown in Fig. 3.
2	Save the Configuration Matrix: Before proceeding with programming, save the current configuration matrix to preserve any existing settings and configurations. This serves as a backup in case any changes need to be reverted.
3	Insert and Name a New CFC Chart: Create a new CFC and assign it a descriptive name that reflects its purpose or function within the relay's logic. This chart will contain the logic and control functions for the adaptive OCR scheme
4	Draw the Chart: Design the CFC chart by adding function blocks and defining their interconnections. Use the graphical interface provided by DIGSI CFC to visually represent the logic of the adaptive OCR scheme. Ensure that the chart is logically structured and easy to understand, as shown in Fig. 4.
5	Shift the Chart to the Proper Priority Class: Assign the CFC chart to the appropriate priority class based on its importance and execution sequence within the relay's control logic. Priority classes determine the order in which different charts are executed during runtime, as shown in Fig. 4.
6	Verify the Run Sequence: Validate the run sequence of the CFC chart to ensure that the logic flows correctly and that there are no conflicts or errors. Verify that the chart operates as intended under various fault and operating conditions, as shown in Fig. 5.
7	Compile the Chart: Compile the CFC chart to generate the executable code that will be loaded onto the relay. The compilation process checks for syntax errors and converts the graphical logic into machine-readable instructions, as shown in Fig. 6.
8	Save and Download the Parameter Set: Save the completed parameter set and download it to the relay. This transfers the programmed logic and settings to the relay's memory, making them available for execution during operation. Verify that the relay acknowledges the successful download and is ready for operation.

misoperations can be by cyberattacks, which exploit security vulnerabilities in software and communication channels. When cyberattacks successfully breach protection systems, they can cause relays to operate erratically due to inadequate authentication measures. This irregular behavior can expose the safety and reliability of power systems. Understanding the impact of such malicious activities on power system operations is crucial to mitigate risks and enhance system security (Shih et al., 2017; El-Naily et al., 2022). When an OCR is compromised by an attacker, it can lead to significant disruptions in power injections and load demand, potentially resulting in parts of the grid being disconnected from the main system. A compromised relay can change the topology of the power grid, thereby causing instability and irregular operation. Distinguishing between the normal operation of overcurrent relays in response to short circuit faults and their behavior due to cyberattacks is particularly challenging.

This makes it essential to consider the digital OCR scheme as a critical component for exploring and analyzing the vulnerabilities associated with various attack scenarios on relay operation. This work develops two group settings for OCRs, as shown in Table 3, to protect the power system from cyber attacks that might compromise grid stability and minimize the impact of these threats. The proposed novel adaptive OCR approach involves continuous monitoring of electrical parameters (CB and relay current), with real-time communication being a critical component for transmitting OCR signals.

The success of this new adaptive approach relies on the ability of OCRs to automatically adjust their settings in real-time. Unlike previous adaptive schemes that rely only on CB status, as described in Table 3, the proposed approach incorporates not only CB status but also the current contributions throughout the grid. This multifaceted functionality enables the protection system to adapt quickly and correctly to varying grid conditions using four group settings, as outlined in Table 3. This flexibility enhances the reliability and efficiency of OCR coordination. This approach ensures that the protection system can respond to both routine changes in grid configuration and unexpected events such cyber attack on CBs, thus improving the overall stability and resilience of power systems.

In general, the proposed method serves as a solution to the challenges posed by cyber-attacks on adaptive protection systems. It is designed for implementation on digital relays, following to programming standards such as IEC 61131–3. However, it is not applicable to static relays due to their inherent limitations in programmability and compatibility with adaptive techniques. Additionally, the programming requirements may necessitate specific expertise and resources, potentially increasing the complexity and cost of deployment. However, smart grids heavily rely on robust communication infrastructure, which serves as a critical part for real-time data exchange and coordination among

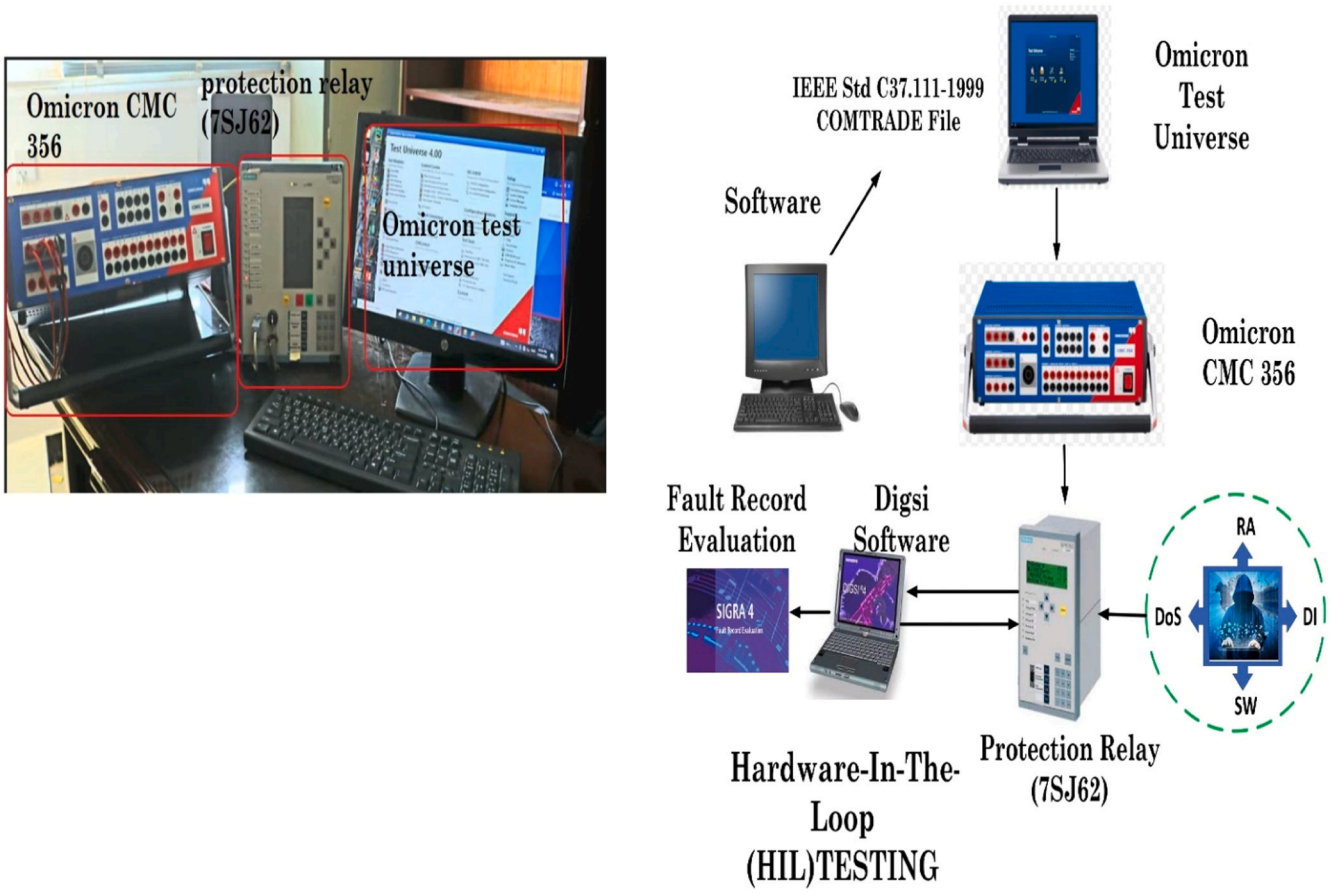


Fig. 7. The overall architecture of cyber-physical power protection system testbed.

devices. In the event of a communication circuit failure within the smart grid context, the proposed adaptive OCR scheme incorporates contingency measures to ensure continued operational reliability. During communication failures or emergency scenarios in the electrical grid, our adaptive OCR scheme is designed to automatically adjust its settings to Group D. This configuration ensures that protection devices can operate effectively even in the absence of real-time communication. The decision-making process for switching to Group D setting. By integrating adaptive strategies that accommodate communication failures, our approach enhances the resilience of power systems. It ensures that critical protection functions remain active and responsive, mitigating potential risks associated with extended communication outages. The proposed adaptive OCR scheme not only optimizes grid performance under normal operating conditions but also includes robust contingency plans for communication failures. This capability highlights its reliability in maintaining grid stability and protecting against potential disruptions in smart grid environments.

In general, each OCR protection devices continually measures current and voltage from the electrical grid. In the proposed method, data handling ensures that the stored or measured data used for decision-making is more reliable to spam or erroneous information. The OCR, Siemens 7SJ62 protection device, incorporates four groups tailored for different operational modes and based on different status and measurements. Each group's settings for fault current calculations and trip times are predefined and securely stored within the device. To guarantee the integrity of stored data, our method employs stringent validation processes. Data stored within the protection device is periodically updated and verified against real-time measurements and grid conditions. This verification process ensures that the data used for protection decisions accurately reflects the current state of the electrical grid and mitigates the risk of using outdated or falsified information.

3. Cyber-physical threats to adaptive protection schemes

Overcurrent Relays (OCRs) are critical components for ensuring the reliable operation of electrical power systems by clearing faults within their designated protection zones. To achieve proper coordination, these relays typically include a backup mechanism located upstream from the primary protection. However, in DN with multiple DER locations, ensuring effective protection becomes more complicated. Constant changes in grid topology, generation patterns, and load demand necessitate adaptive OCR systems, as traditional protection schemes often fall short (Alasali et al., 2021a, 2021b). However, adaptive OCR systems are vulnerable to cyber-physical threats that can compromise their performance and reliability. For example, a cyberattack could change the adaptive relay settings, leading to miscoordination or improper relay operations. An attack could also block the relay's trip signal or disrupt communication links, preventing the relay from isolating a fault, potentially leading to broader system failures. These threats could cause healthy lines to be isolated, resulting in power outages, damage to equipment, and disconnection of DERs. Fig. 1 presents potential cyber-physical threats on the adaptive protection scheme.

- Switching Attack (SW): Switching attacks refer to malicious interference with the operation of CBs, usually by manipulating relay tripping functions. These attacks can cause unexpected changes in the mode of operation for CBs, leading to unintended power system behavior. A random switching vector is used to define the switching attack, where this vector specifies the timing and status for opening or closing specific CBs. Furthermore, this vector indicates which

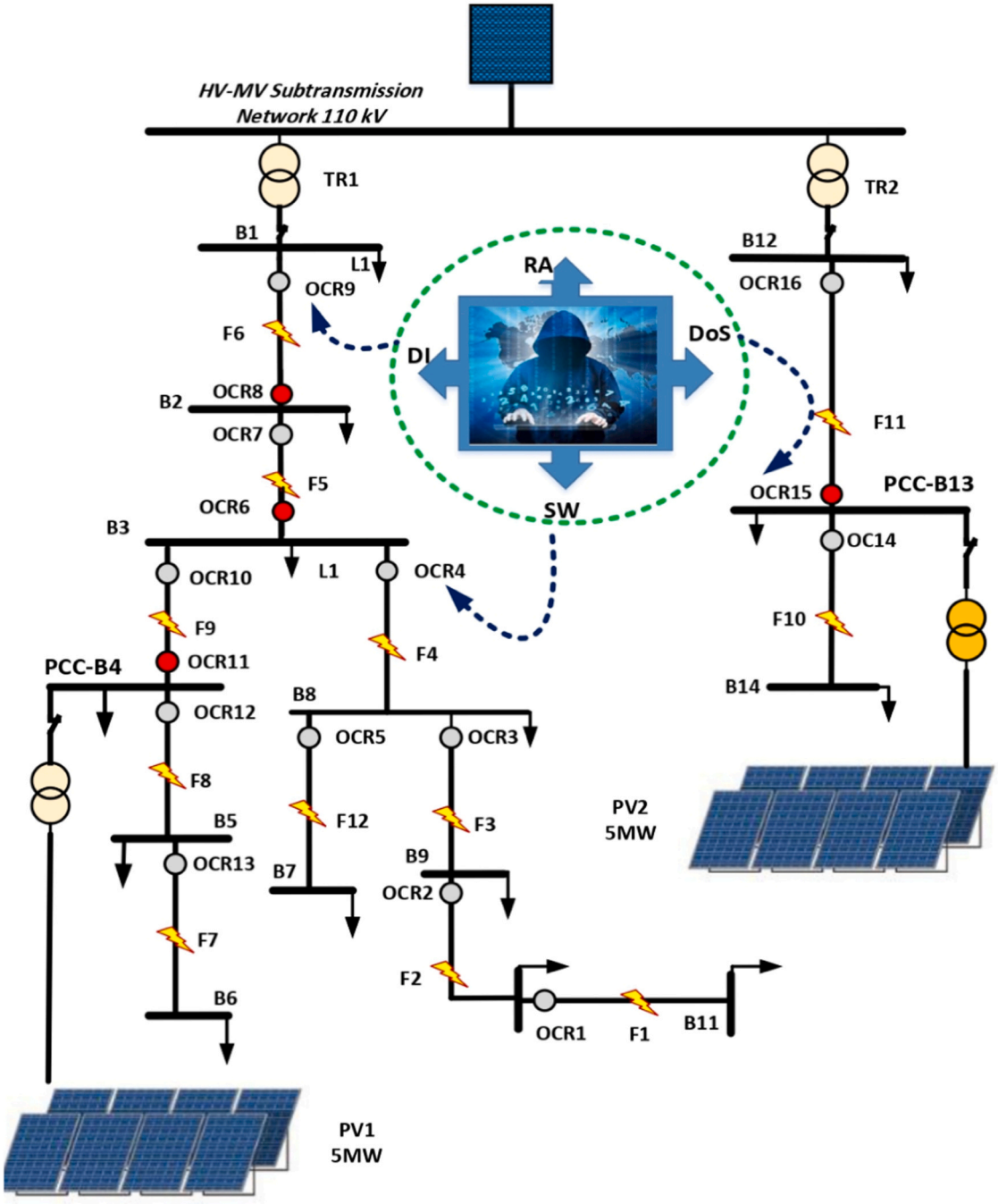


Fig. 8. CIGRE distribution network and potential cyber-physical threats.

breakers are to be opened or closed during an attack. A malicious switching attack can allow an external adversary to gain access to the control functions of digital relays that manage critical CBs, like those that govern tie-line connections between grid segments or that protect a generator substation. If an attacker manipulates these relay control functions, it can lead to several detrimental outcomes, such as disconnecting a generator substation from the rest of the network or disabling specific interconnectors between different grid areas. These actions can significantly disrupt power flow across the grid, potentially causing power outages, grid instability, or even large-scale blackouts. Switching attacks can be particularly insidious because they target key components of the power grid's control infrastructure. An attacker with access to digital relay control functions can create widespread disruption by altering the operational state of CBs, leading to cascading failures. To protect against such attacks, power systems need robust security measures, including secure communication channels, strong authentication protocols, and real-time monitoring to detect unauthorized changes in CB status or relay settings. Additionally, redundancy and backup mechanisms can help ensure system resilience against switching attacks and maintain stable power flow even in the face of malicious interference (Mukherjee, 2022; Liu et al., 2014).

- Denial of Service (DoS) Attack: Interlocking is a critical safety feature in digital substations designed to ensure the safe operation of switchgear equipment. This safety mechanism employs a software-based scheme that relies on the IEC 61850 GOOSE (Generic Object-Oriented Substation Event) protocol to exchange information between control units in different parts of the substation. A DoS

Table 5
The I_p and CTR for each OCR.

OCR	Group Setting A	Group Setting B	Group Setting C	Group Setting D
	I_p			
OCR1	100	100	100	50
OCR2	100	100	100	50
OCR3	100	100	100	50
OCR4	100	100	100	50
OCR5	100	100	100	50
OCR6	100	100	100	50
OCR7	150	150	150	50
OCR8	100	100	100	50
OCR9	200	200	200	50
OCR10	100	100	100	50
COR11	100	100	100	50
OCR12	100	100	100	50
OCR13	100	100	100	50
OCR14	100	100	100	50
OCR15	100	100	100	50
OCR16	100	100	100	50

Table 6
The TMS for each adaptive OCR at all group settings.

OCR	Group Setting A TMS	Group Setting B	Group Setting C	Group Setting D
OCR1	0.05	0.05	0.05	0.05
OCR2	0.17	0.165	0.12	0.14
OCR3	0.285	0.32	0.241	0.265
OCR4	0.4	0.432	0.33	0.4
OCR5	0.05	0.05	0.05	0.05
OCR6	0.43	0.095	0.095	0.125
OCR7	0.43	0.446	0.27	0.472
OCR8	0.47	0.05	0.05	0.05
OCR9	0.47	0.482	0.265	0.6
OCR10	0.282	0.278	0.192	0.278
COR11	0.282	0.142	0.142	0.2
OCR12	0.162	0.168	0.14	0.15
OCR13	0.05	0.05	0.05	0.05
OCR14	0.05	0.05	0.05	0.5
OCR15	0.182	0.05	0.01	0.05
OCR16	0.182	0.182	0.1	0.182

attack occurs when an attacker aims to disrupt or exploit relay services to prevent them from performing essential functions. In a DoS attack, the attacker overcomes the system's communication resources, reducing the availability of the data used for normal operations, thereby causing the system to become unresponsive to other service requests. Two common policies for DoS attacks in digital substations are (Jahromi et al., 2020):

- Attack Policy (1): Blocking Relay Operations: This type of DoS attack involves transmitting malicious information to targeted digital relays, disrupting their normal operation. By compromising the communication between relays and local CBs, this attack prevents protective devices from functioning during credible contingencies. This results in control commands or breaker reclosing commands failing to execute, leading to a lack of response during fault events or other grid disturbances. For instance, when the relay's control logic or reclosing instruction is disrupted, local CBs may not open during a fault, resulting in significant system damage or wider outages.
- Attack Policy (2): Delaying Relay Responses: In this scenario, a DoS attack keeps relays in an idle state for a specified period, preventing them from responding to any disturbance event. This attack policy can either prevent the relay from issuing a trip signal to open CBs during a fault or delay the transmission of control commands to close or re-close the CBs once the fault is cleared. By delaying or inhibiting critical relay functions, this attack can cause extended system instability, leading to broader impacts on the grid. Given the risks posed by DoS attacks, it is imperative to implement robust security measures in digital substations. This includes securing communication channels, employing redundancy in critical systems, and establishing monitoring mechanisms to detect and respond to abnormal activity. Further, it's essential to have contingency plans in place to ensure that the grid can maintain operational stability even in the event of a DoS attack, reducing the potential for widespread damage or outages (Amin et al., 2020; Liu et al., 2014).

- Replay Attack: A replay attack is a deceptive approach in which legitimate data is captured and then maliciously retransmitted at a later time. In this type of attack, an adversary can repeat data recorded from a compromised source, such as a database or data logger, to simulate an event that has already occurred. Attackers might intercept network traffic and collect valid data, such as the output from a digital fault recorder or CB status logs over a certain period. They can then resend this previously recorded information to trigger a specific response in the power system, potentially causing unintended consequences such as false tripping of CBs and unplanned power outages. Replay attacks introduce significant risks because they can manipulate system operations without any modification to the data content, making them challenging to detect. The attacker might resend disturbance data or control signals to trick the power system into thinking an event is recurring, prompting the system to react inappropriately. For example, a CB could be instructed to open based on data that was accurate in the past but no longer reflects the current state of the system, leading to a sudden power interruption. This type of attack can be especially harmful because it exploits the timing constraints within CB operations. Without careful examination of data timestamps and verification of the context in which the data was generated, replay attacks can go unnoticed, causing disruptions that appear to be legitimate operational events. The effectiveness of these attacks relies on the ability to replicate past events to manipulate system responses, which could lead to broader instability and system damage. To defend against replay attacks, power systems should implement robust security measures such as secure communication protocols with time-stamping and message authentication mechanisms. Additionally, systems should incorporate intrusion detection techniques that can recognize abnormal patterns in network traffic and flag suspicious activity. By ensuring data integrity and verifying the authenticity of transmitted signals, the risk of successful replay attacks can be significantly reduced, safeguarding the stability and reliability of the power system (Mukherjee, 2022; Jahromi et al., 2020).
- Data Integrity attack (DI): A DI involves injecting false commands or data to disrupt the normal operation of digital protection relays, potentially compromising their integrity. These attacks aim to manipulate the control logic of relays, leading to erroneous responses that can jeopardize the stability and safety of the power system. By injecting incorrect data or control commands, attackers can cause digital protection relays to behave unpredictably. For example, an

Table 7
The TMS for each adaptive OCR at all group settings.

Fault location	Relay	Group setting A		Group setting B		Group setting C		Group setting D	
		Fault current (A)	Tripping time (seconds)	Fault current (A)	Tripping time (seconds)	Fault current (A)	Tripping time (seconds)	Fault current (A)	Tripping time (seconds)
F1	OCR1	1254	0.13	1434	0.128	723	0.173	1434	0.11
F1	OCR2	1254	0.43	1434	0.442	723	0.41	1434	0.31
F2	OCR2	1310	0.45	1495	0.41	806	0.39	1495	0.31
F2	OCR3	1310	0.75	1495	0.806	806	0.79	1495	0.60
F3	OCR3	1407	0.73	1598	0.786	832	0.78	1598	0.60
F3	OCR4	1407	1.03	1598	1.061	832	1.07	1598	0.90
F4	OCR4	1452	1.019	1641	1.051	843	1.06	1641	0.907
F4	OCR6	1452	1.29	1432	1.353	586	1.36	1432	1.208
F4	OCR7	1452	1.29	289	0.621	289	0.62	289	0.49
F5	OCR7	1667	1.22	289	0.928	289	0.92	289	0.78
F5	OCR8	1667	1.519	1697	1.262	635	1.29	1679	1.13
F5	OCR9	1667	1.519	1697	1.552	635	1.58	1679	1.44
F6	OCR9	3343	1.136	3392	1.158	691	1.47	3392	1.13
F7	OCR13	1274	0.13	289	0.327	289	0.32	289	0.19
F7	OCR12	1274	0.43	289	0.621	289	0.62	289	0.49
F8	OCR12	1472	041	1467	0.127	804	0.16	1467	0.11
F8	OCR11	1472	0.71	1467	0.42	804	0.46	1467	0.34
F8	OCR10	1472	0.71	1721	0.402	856	0.44	1721	0.34
F9	OCR10	1560	0.69	1466	0.705	599	0.73	1466	0.63
F9	OCR7	1560	1.25	1570	0.687	620	0.73	1570	0.63
F10	OCR14	2119	0.13	1570	1.298	620	1.3	1570	1.16
F10	OCR15	2119	0.413	289	0.928	289	0.92	289	0.78
F10	OCR16	2119	0.413	2327	0.113	927	0.15	2327	0.11
F11	OCR15	3046	0.413	2044	0.413	668	0.36	2044	0.41
F11	OCR16	289	0.113	289	0.113	289	0.32	289	0.19
F12	OCR5	1245	0.11	3082	0.413	678	0.35	3082	0.41
F12	OCR4	1245	1	1424	0.113	722	0.12	1424	0.11

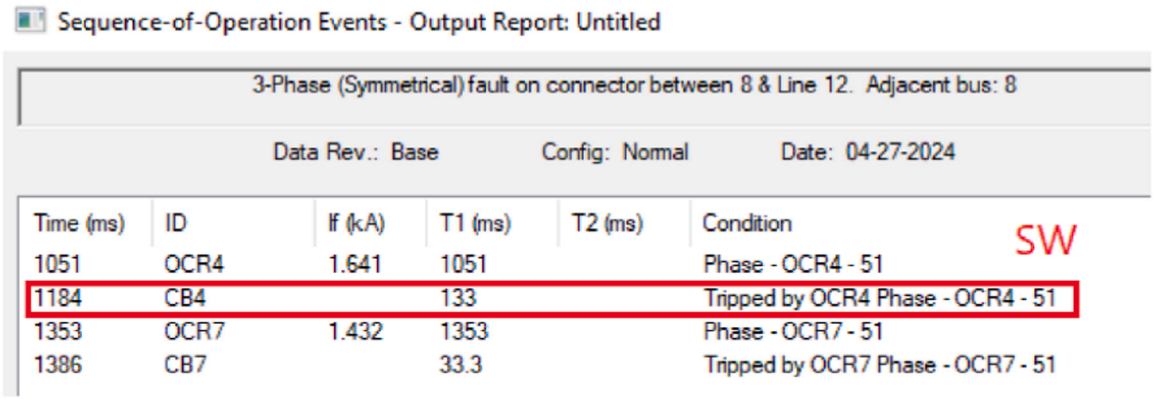


Fig. 9. Switching attacks on OCR4.

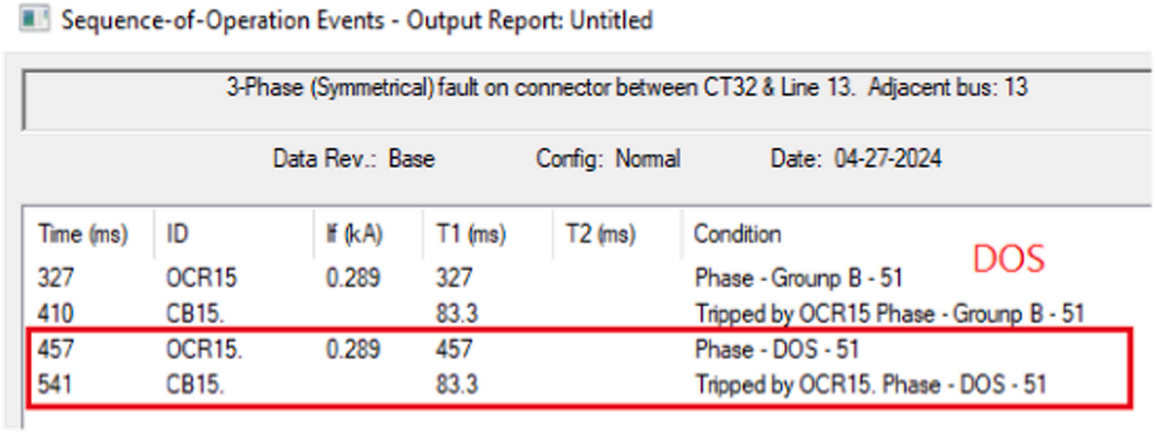
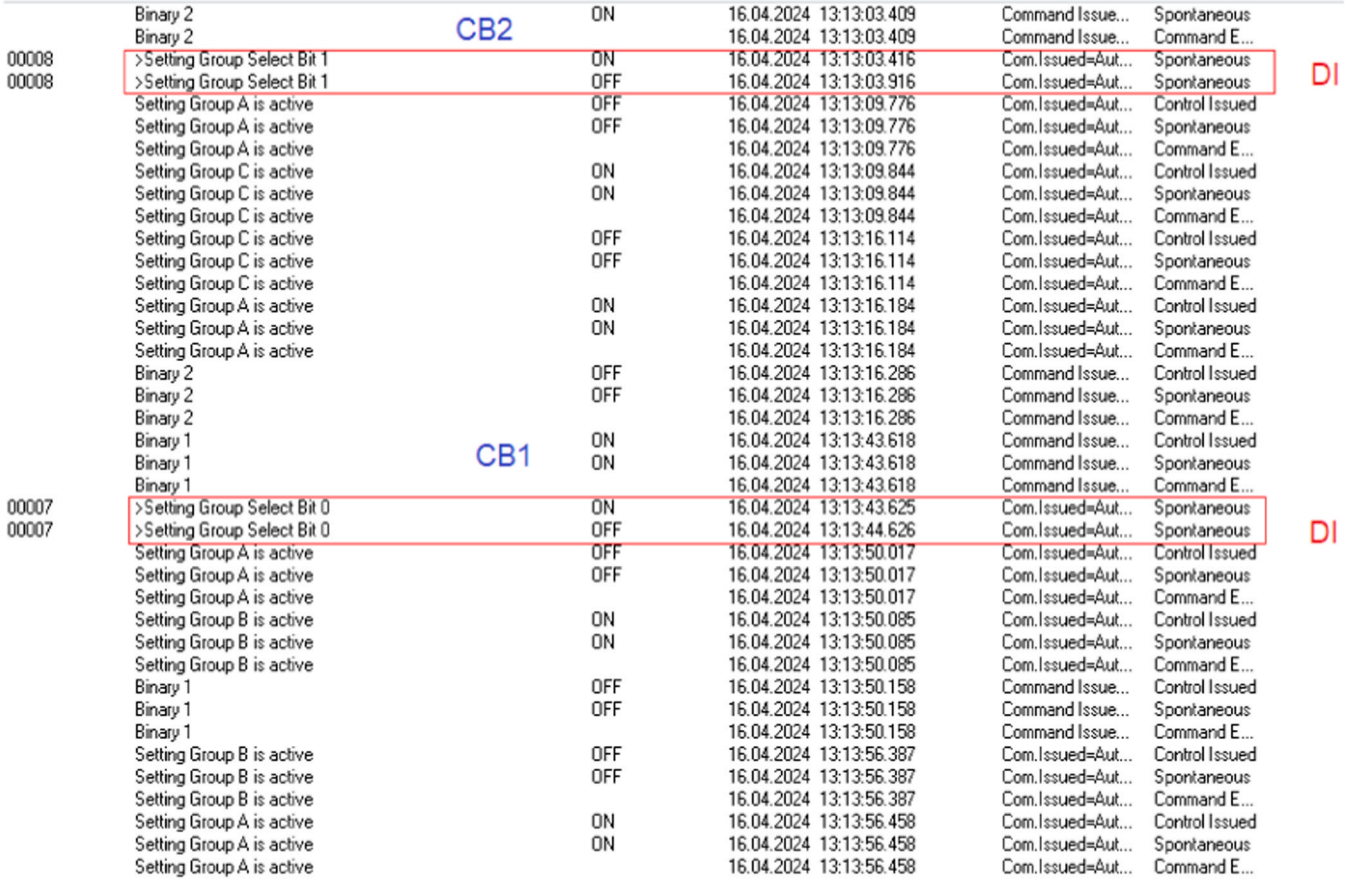


Fig. 10. DoS attack on OCR15.



	Binary 2	ON	16.04.2024 13:13:03.409	Command Issue...	Spontaneous
	Binary 2		16.04.2024 13:13:03.409	Command Issue...	Command E...
00008	>Setting Group Select Bit 1	ON	16.04.2024 13:13:03.416	Com.Issued=Aut...	Spontaneous
00008	>Setting Group Select Bit 1	OFF	16.04.2024 13:13:03.916	Com.Issued=Aut...	Spontaneous
	Setting Group A is active	OFF	16.04.2024 13:13:09.776	Com.Issued=Aut...	Control Issued
	Setting Group A is active	OFF	16.04.2024 13:13:09.776	Com.Issued=Aut...	Spontaneous
	Setting Group A is active		16.04.2024 13:13:09.776	Com.Issued=Aut...	Command E...
	Setting Group C is active	ON	16.04.2024 13:13:09.844	Com.Issued=Aut...	Control Issued
	Setting Group C is active	ON	16.04.2024 13:13:09.844	Com.Issued=Aut...	Spontaneous
	Setting Group C is active		16.04.2024 13:13:09.844	Com.Issued=Aut...	Command E...
	Setting Group C is active	OFF	16.04.2024 13:13:16.114	Com.Issued=Aut...	Control Issued
	Setting Group C is active	OFF	16.04.2024 13:13:16.114	Com.Issued=Aut...	Spontaneous
	Setting Group C is active		16.04.2024 13:13:16.114	Com.Issued=Aut...	Command E...
	Setting Group A is active	ON	16.04.2024 13:13:16.184	Com.Issued=Aut...	Control Issued
	Setting Group A is active	ON	16.04.2024 13:13:16.184	Com.Issued=Aut...	Spontaneous
	Setting Group A is active		16.04.2024 13:13:16.184	Com.Issued=Aut...	Command E...
	Binary 2	OFF	16.04.2024 13:13:16.286	Command Issue...	Control Issued
	Binary 2	OFF	16.04.2024 13:13:16.286	Command Issue...	Spontaneous
	Binary 2		16.04.2024 13:13:16.286	Command Issue...	Command E...
	Binary 1	ON	16.04.2024 13:13:43.618	Command Issue...	Control Issued
	Binary 1	ON	16.04.2024 13:13:43.618	Command Issue...	Spontaneous
	Binary 1		16.04.2024 13:13:43.618	Command Issue...	Command E...
00007	>Setting Group Select Bit 0	ON	16.04.2024 13:13:43.625	Com.Issued=Aut...	Spontaneous
00007	>Setting Group Select Bit 0	OFF	16.04.2024 13:13:44.626	Com.Issued=Aut...	Spontaneous
	Setting Group A is active	OFF	16.04.2024 13:13:50.017	Com.Issued=Aut...	Control Issued
	Setting Group A is active	OFF	16.04.2024 13:13:50.017	Com.Issued=Aut...	Spontaneous
	Setting Group A is active		16.04.2024 13:13:50.017	Com.Issued=Aut...	Command E...
	Setting Group B is active	ON	16.04.2024 13:13:50.085	Com.Issued=Aut...	Control Issued
	Setting Group B is active	ON	16.04.2024 13:13:50.085	Com.Issued=Aut...	Spontaneous
	Setting Group B is active		16.04.2024 13:13:50.085	Com.Issued=Aut...	Command E...
	Binary 1	OFF	16.04.2024 13:13:50.158	Command Issue...	Control Issued
	Binary 1	OFF	16.04.2024 13:13:50.158	Command Issue...	Spontaneous
	Binary 1		16.04.2024 13:13:50.158	Command Issue...	Command E...
	Setting Group B is active	OFF	16.04.2024 13:13:56.387	Com.Issued=Aut...	Control Issued
	Setting Group B is active	OFF	16.04.2024 13:13:56.387	Com.Issued=Aut...	Spontaneous
	Setting Group B is active		16.04.2024 13:13:56.387	Com.Issued=Aut...	Command E...
	Setting Group A is active	ON	16.04.2024 13:13:56.458	Com.Issued=Aut...	Control Issued
	Setting Group A is active	ON	16.04.2024 13:13:56.458	Com.Issued=Aut...	Spontaneous
	Setting Group A is active		16.04.2024 13:13:56.458	Com.Issued=Aut...	Command E...

Fig. 11. DI attack on OCR9.

attacker might send a false signal to a relay, causing it to trip a circuit breaker unnecessarily, leading to unplanned power outages or compromising the protection scheme's effectiveness. Integrity attacks can be challenging to detect because they may not produce immediate or visible effects. They can slightly change relay behavior, resulting in delayed or early operations that can destabilize the grid. These attacks are particularly concerning in smart grids, where digital communication and automation play a central role in relay coordination and control.

The effectiveness of this work in mitigating cyber-physical attacks is supported by a HIL validation test and detailed case study illustrating its performance under various scenarios. The proposed adaptive OCR scheme incorporates advanced features that enhance resilience against cyber threats, including SW, DoS, DI and reply attacks. In the following section, Section 4, our study implements the adaptive protection scheme on a realistic industrial relay, specifically the Multifunction Protection Relay SIEMENS 7SJ62. This implementation is validated using a sophisticated cyber-power protection testbed, which integrates HIL and controller-in-the-loop capabilities. In Section 5, the proposed adaptive protection scheme employed on a CIGRE distribution network, aiming to optimize OCR coordination and minimize tripping time. This setup allows us to simulate and evaluate the performance of OCR coordination and response under controlled cyber-attack scenarios.

- Real-time Adaptive Adjustment: Unlike previous schemes primarily relying on CB status, the proposed approach dynamically adjusts OCR settings based on real-time grid parameters, including CB status and current contributions throughout the grid. This capability ensures swift response and adaptation to changes in grid topology caused by cyber-physical attacks.
- Comprehensive Evaluation: The validation process involves creating detailed models of the power system elements within the testbed, including commercial hardware and software components. This holistic approach enables us to measure the system's robustness against cyber threats across various operational conditions.
- Performance Under Attack Scenarios: Simulations of significant cyber-attack scenarios, such as network intrusion and data falsification, assess how the adaptive OCR scheme mitigates potential vulnerabilities. Demonstrating resilience in these scenarios provides concrete evidence of its effectiveness in maintaining power system stability and reliability.

In conclusion, the HIL and case study simulation results highlight the capability of the proposed adaptive OCR scheme to perform effectively under cyber-physical attacks.

4. Cyber-physical power protection system testbed

4.1. Verification in industrial relays

Validation was conducted by implementing the proposed novel adaptive protection scheme, as presented in Section 2.2, on an industrial relay, specifically the Multifunction Protection Relay SIEMENS 7SJ62. The validation process involved utilizing various tools to create detailed models representing different elements of the power system, as shown in Fig. 2:

- Network Structure Implementation: The standard DN model, including CIGRE distribution network configurations with and without Photovoltaic (PV) systems, was constructed using ETAP and ATP/EMTP simulations.

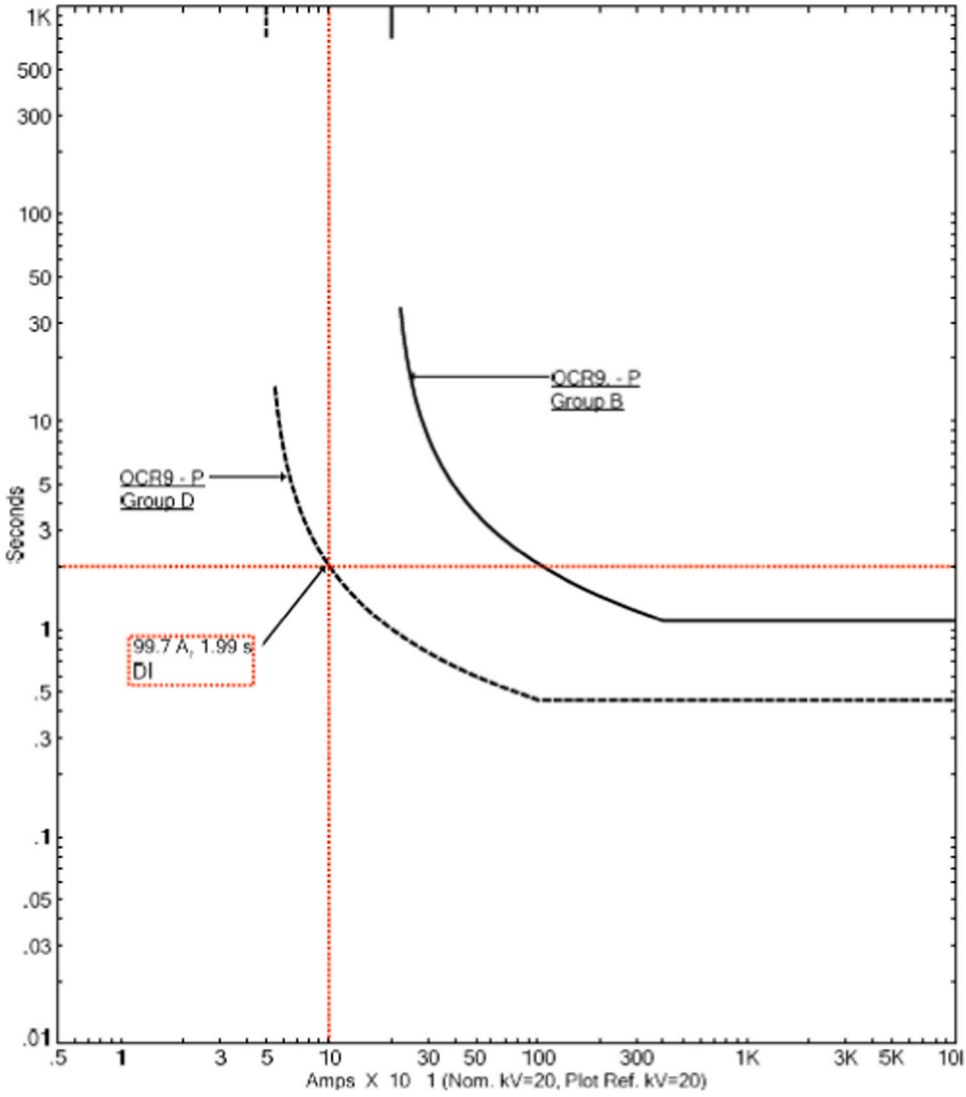
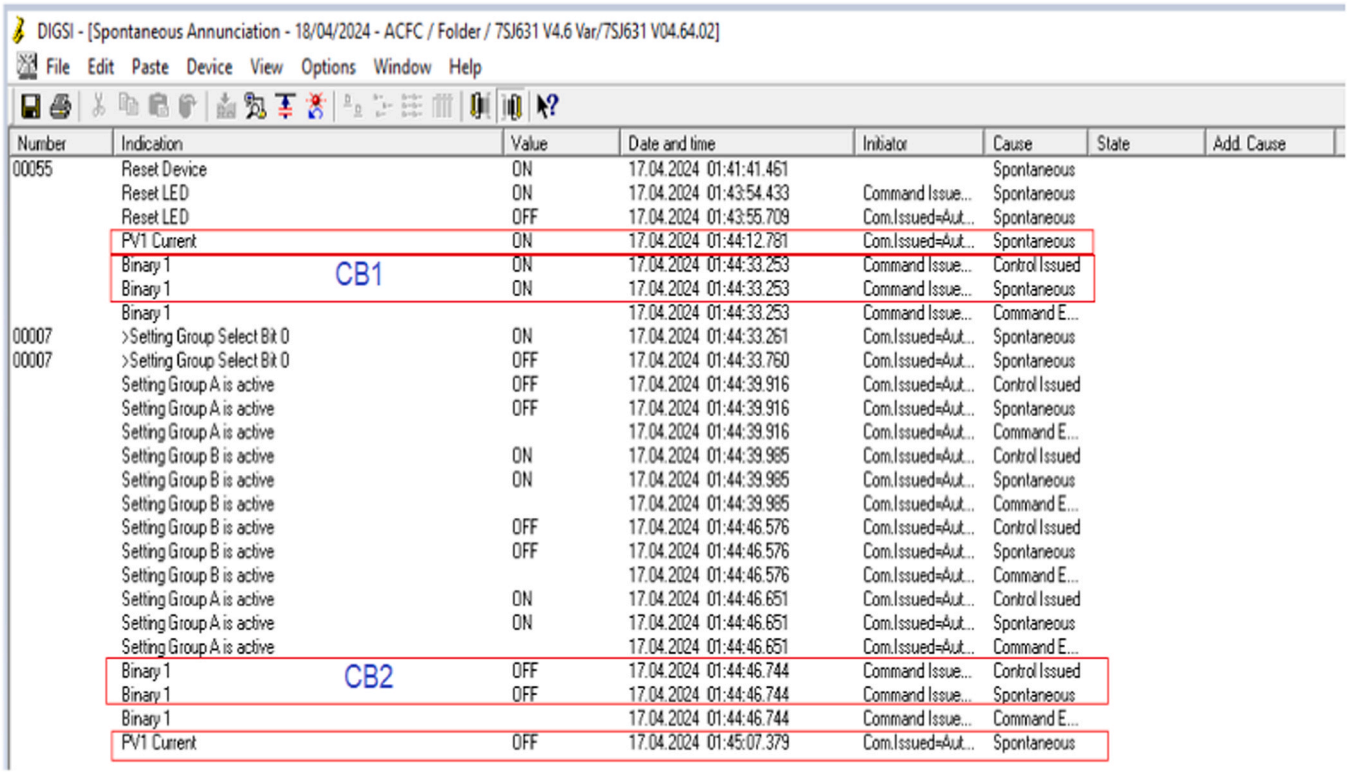


Fig. 12. The current-time curves of OCR9 under DI attack.

- Initial group setting is determined based on the network topology and current values.
- Load Flow Calculation: A load flow analysis, employing the Newton-Raphson method, was performed to determine the initial current settings for each Overcurrent Relay (OCR) and to initialize relay settings.
- Short Circuit Calculation: Short circuit calculations were conducted based on IEC 60909 standards in diverse scenarios to evaluate fault conditions.
- Optimization Techniques Application: The configuration for the OCR system was determined using robust optimization methods such as the Water Cycle Algorithm (WCA), depending on the prevailing fault conditions. These techniques effectively addressed OCR coordination challenges.
- Verification of the Setting: The programming of automation functions in SIPROTEC devices was accomplished using DIGSI CFC (Continuous Function Chart), which is a component of DIGSI 4 software. This graphic user interface facilitated the connection of information items and programming of interlocks and switching sequences. Additionally, it allowed for the editing of measured values and generation of messages. SIPROTEC devices feature rear serial interfaces for connection to a control system via the IEC 61131–3 standard. Protective relays have evolved to resemble programmable logic controllers (PLCs) (Xiong et al., 2020; Cavalieri and Salafia, 2020), providing comprehensive control-based operations and electrical asset protection. Utilizing an established format based on the IEC 61131–3 programming standard, solutions have been devised employing CFC conventions. In contrast to general-purpose computer programs, PLC programs typically undergo cyclical execution, comprising three phases: input, execution, and output. Each cycle involves reading values from input ports, executing the program code with these input values, and then flushing the values out to physical output ports. The cyclic nature of PLC programs, coupled with potential dependencies on previous cycles, necessitates special consideration for program verification to ensure accurate analysis.

Utilizing a CFC based representation of logic offers a more intuitive method for comparison by examining the instance number of function blocks and their connections. CFC provides a digital worksheet-based representation that not only offers the aforementioned benefits to relay users but also facilitates troubleshooting and testing. Additionally, it enables the provision of an online view of the logical statuses of each element involved. When programming functions with DIGSI CFC, the following eight steps should be followed consecutively, as outlined in Table 4:



Number	Indication	Value	Date and time	Initiator	Cause	State	Add. Cause
00055	Reset Device	ON	17.04.2024 01:41:41.461		Spontaneous		
	Reset LED	ON	17.04.2024 01:43:54.433	Command Issue...	Spontaneous		
	Reset LED	OFF	17.04.2024 01:43:55.709	Com.Issued=Aut...	Spontaneous		
	PV1 Current	ON	17.04.2024 01:44:12.781	Com.Issued=Aut...	Spontaneous		
	Binary 1	ON	17.04.2024 01:44:33.253	Command Issue...	Control Issued		
	Binary 1	ON	17.04.2024 01:44:33.253	Command Issue...	Spontaneous		
	Binary 1		17.04.2024 01:44:33.253	Command Issue...	Command E...		
00007	>Setting Group Select Bit 0	ON	17.04.2024 01:44:33.261	Com.Issued=Aut...	Spontaneous		
00007	>Setting Group Select Bit 0	OFF	17.04.2024 01:44:33.760	Com.Issued=Aut...	Spontaneous		
	Setting Group A is active	OFF	17.04.2024 01:44:39.916	Com.Issued=Aut...	Control Issued		
	Setting Group A is active	OFF	17.04.2024 01:44:39.916	Com.Issued=Aut...	Spontaneous		
	Setting Group A is active		17.04.2024 01:44:39.916	Com.Issued=Aut...	Command E...		
	Setting Group B is active	ON	17.04.2024 01:44:39.985	Com.Issued=Aut...	Control Issued		
	Setting Group B is active	ON	17.04.2024 01:44:39.985	Com.Issued=Aut...	Spontaneous		
	Setting Group B is active		17.04.2024 01:44:39.985	Com.Issued=Aut...	Command E...		
	Setting Group B is active	OFF	17.04.2024 01:44:46.576	Com.Issued=Aut...	Control Issued		
	Setting Group B is active	OFF	17.04.2024 01:44:46.576	Com.Issued=Aut...	Spontaneous		
	Setting Group B is active		17.04.2024 01:44:46.576	Com.Issued=Aut...	Command E...		
	Setting Group A is active	ON	17.04.2024 01:44:46.651	Com.Issued=Aut...	Control Issued		
	Setting Group A is active	ON	17.04.2024 01:44:46.651	Com.Issued=Aut...	Spontaneous		
	Setting Group A is active		17.04.2024 01:44:46.651	Com.Issued=Aut...	Command E...		
	Binary 1	OFF	17.04.2024 01:44:46.744	Command Issue...	Control Issued		
	Binary 1	OFF	17.04.2024 01:44:46.744	Command Issue...	Spontaneous		
	Binary 1		17.04.2024 01:44:46.744	Command Issue...	Command E...		
	PV1 Current	OFF	17.04.2024 01:45:07.379	Com.Issued=Aut...	Spontaneous		

Fig. 13. Proposed novel adaptive protection under DI attack.

4.2. Hardware-in-the-loop test

In general, a testbed functions as an experimental environment equipped with state-of-the-art technology to construct test systems or equipment. Its purpose is to validate concepts, products, systems, and technologies related to digital transformation. Testbeds serve a variety of purposes including education, demonstration, research, development, and invention projects, primarily aimed at assessing specific tasks. Moreover, they offer comprehensive evaluation protocols for both hardware and software aspects, providing valuable insights across various study disciplines. This section delves into the design and execution of a sophisticated cyber-power protection testbed, amalgamating simulation and real devices within a modular framework. The testbed comprises commercial hardware, software, and simulated devices for data measurement and collection, ensuring a holistic approach to testing and evaluation. The testbed incorporates HIL and controller-in-the-loop capabilities, enabling seamless connection and communication with real hardware controllers such as the OMICRON-256 and relays. This setup allows for the evaluation of OCRs protection schemes within a microgrid environment at an early stage, leveraging the practicality provided by real hardware components. The overall architecture of the testbed is depicted in Fig. 7. In the experimental study, the performance of a Multifunction Protection Relay SIEMENS 7SJ62, installed within the real power electrical network, is compared with a relay parameter determined by ATP/EMTP software. The parameters of the SIEMENS 7SJ62 are configured using the DIGSI Software, an engineering tool specifically designed for programming SIPROTEC SIEMENS protection relays. To assess and validate the proposed relay, the study employs the OMICRON-256 to replay fault events recorded in a simplified power system simulated within ATP/EMTP software, transmitting them to the SIEMENS 7SJ62 relay for analysis. The laboratory test setup encompasses simulations of relay operation and the application of adaptive protection schemes derived from ATP/EMTP software. In the experimental setup, current signal channels are injected into the OMICRON-256 test device from both primary and secondary terminals. These signals are then transmitted to the relay for analysis. The response of the relay to both external and internal faults is examined through simulations conducted using ATP-EMTP software. Subsequently, current signals captured from current transformers within the simulated model are fed back into the OMICRON-256 test device. These signals are observed through a fault recorder in the DIGSI software, facilitating further analysis.

5. Resilience evaluation of adaptive protection systems

Adaptive power protection systems are essential for the secure and reliable operation of smart grid infrastructures. They are responsible for detecting and isolating faults and abnormal operating conditions within smart grid. However, due to their reliance on digital communication technology, they are vulnerable to cyber-attacks that could compromise their functionality and disrupt network operations. Attacks on OCRs can result in physical damage, operational disruptions, and power outages. To mitigate these risks, it is essential for power network operators to assess the resilience of DNs with DERs and modern adaptive OCRs under various cyber-physical threats. To evaluate the resilience of traditional and proposed novel adaptive OCR performance in DN, focusing on sensitivity and selectivity. Key assessment terms include:

- Healthy line outages, representing energy not supplied during disruptions.
- Tripping time and miscoordination events under different fault and cyber threat scenarios.

By evaluating the resilience of adaptive OCRs in DN with DERs across various cyber-physical threat scenarios, we can identify vulnerabilities and enhance the security posture of power networks to ensure uninterrupted and reliable electricity supply. The proposed method addresses the challenge of frequent changes in load and grid configurations, particularly in the context of renewable energy integration both on-grid and off-grid scenarios. This adaptability is crucial

for maintaining grid stability amidst dynamic power fluctuations and operational modes. The proposed adaptive OCR approach introduced in this study includes four group settings, as described in Table 3, tailored to handle varying conditions influenced by renewable energy sources, such as photovoltaic (PV) systems. Table 3 outlines these settings, which consider PV current contributions and the status of utility and PV power sources. This configuration is essential for optimizing OCR performance during transitions between grid-connected and islanded modes, ensuring reliable operation under diverse load profiles and renewable energy inputs. To validate the effectiveness of our approach, simulations were conducted using detailed models of a CIGRE distribution network with PV system integration. These simulations, performed with tools ETAP and ATP/EMTP, encompassed different fault scenarios to evaluate OCR performance across different grid configurations conditions. This included assessing total tripping times under optimal fault management strategies.

By incorporating both on-grid and off-grid renewable energy contexts into the adaptive OCR scheme, our research demonstrates its capability to enhance grid resilience and stability. This approach not only accommodates the variability of renewable energy sources but also mitigates the impact of load and grid configuration changes, thereby advancing the reliability and effectiveness of power system protection.

5.1. Proposed CIGRE grid with adaptive protection scheme and modeling results

The proposed adaptive protection scheme employed on a CIGRE distribution network, depicted in Fig. 8, aiming to optimize OCR coordination and minimize tripping time. The CIGRE grid is constructed based on a 14-bus feeder. Essentially, the grid is powered by a utility HV/M source and protected by 16 OCRs. Additionally, it is linked to two PV units (each rated at 5MVA) via a 1/20 kV set-up transformer, as elaborated further in (Hansen et al., 2017; Habib et al., 2017a). Within the network, three-phase faults are initiated at nodes (F1-F12), representing both near-end and far-end fault locations. For each fault location, two primary OCRs are assigned, with one backup OCR allocated to each primary OCR. The Plug Setting (PS), pickup current (I_p), and Current Transformer Ratio (CTR) for each OCR are detailed in Table 5. Initially, load flow analysis is conducted to ascertain CTR and PS values for each OCR. Furthermore, three-phase short-circuit analysis is performed in accordance with IEC-60909 standards across different locations. The analysis of three-phase short-circuit events is conducted using ETAP software, with relevant data extracted for simulation of the power network model. All necessary OCR data required for the simulation are summarized in Table 6. The network configuration, illustrated in Fig. 8, with a total of 18 OCRs. Detailed specifications regarding the Current Transformer ratio (CT), and optimal Time Multiplier Setting (TMS) for each adaptive OCR are conveniently presented in Table 5 and 6.

In this section, the performance of the proposed adaptive OCR scheme (group setting A, B, C and D) is evaluated across 12 fault location scenarios. The assessment computing the total tripping times for OCR under various fault conditions' locations based on the optimal TMS, as outlined in Table 6. Additionally, a Clearing Time Interval (CTI) of 0.3 seconds is assumed between local and remote backup protection to facilitate rapid coordination between OCRs. As depicted in Table 7, the proposed adaptive OCR approach correctly performs over all grid operation modes. For instance, under F1 conditions, the tripping time of OCR1 was 0.13, 0128, 0173 and 0.11 seconds for group setting A, B, C and D, respectively.

5.2. Adaptive OCRs performance under different Cyber-attack scenarios

In this section, the cybersecurity is explored by simulating different significant cyber-attack scenarios, as illustrated in Fig. 8. The goal is to comprehensively evaluate the performance of traditional recent adaptive protection and the proposed adaptive schemes under various cyber threats. Through this evaluation, insights are required into the resilience and effectiveness of the adaptive protection mechanisms in defending against potential cyber-attacks.

5.2.1. Traditional recent adaptive protection

A common method in adaptive OCR schemes involves adjusting the group relay settings based on the configuration of the network's circuit breakers. This adjustment reflects whether the system is functioning in a conventional mode (with utility sources only) or in a grid-connected mode (incorporating photovoltaic (PV) systems), as discussed in Section 2.1. In this subsection, the objective is to evaluate of the performance of traditional recent adaptive protection scheme under diverse cyber threats.

- Switching Attack (SW): Switching attacks on OCR4 under F4 involve malicious manipulation of CB, by interfering with relay tripping functions, where the OCR4 send the order to trip and CB did not response on time, as shown in Fig. 9.
- Denial of Service (DoS) Attack: DoS attack to disrupt relay services by delaying the tripping signal at OCR15 from 0.327 to 0.427 seconds, as presented in Fig. 10. This will lead to miscoordination events and more thermal stress on the network.
- Data Integrity Attack (DI): DI attack involves the injection of false data about the statues of the CBs to disrupt the group setting operation of OCR, as shown in Fig. 11. The objective of this attack is to manipulate the control logic of relays, where the OCR9 will be adjusted from group B to D. This causes a disconnect signal from relay to CB during normal at 99.7 A, as presented in Fig. 12.

5.2.2. Proposed novel adaptive protection

The proposed adaptive approach enhances the sensitivity of the protection system to the dynamic conditions encountered within the power system, offering a more resilient and adaptable protection mechanism. The significance of the proposed adaptive OCR approach lies in its ability to enhance the resilience of the power system against potential cyber attacks while minimizing their impact. By incorporating real-time monitoring of electrical parameters, such as current and CB status, to dynamically adjust OCR group settings, the system can effectively counteract various attack scenarios. For example, consider a scenario where an attacker attempts DI or DoS attacks, as presented in previous section, to operate the incorrect group setting can be totally avoid by applying the proposed adaptive approach. In the proposed adaptive approach, the OCRs continuously monitor the current and CB status, as shown in Fig. 13. If abnormal behavior indicative of an attack is detected, such as unexpected changes in CB status and without changing in the real currents, the OCRs will not adjust their settings to mitigate the impact of the attack. This could involve adjusting coordination parameters to maintain grid stability and prevent unnecessary outages. This proactive approach not only minimizes the risk of successful attacks but also enhances the overall security attitude of the power system. Overall, the proposed adaptive OCR approach demonstrates the potential to significantly improve the resilience of power systems against cyber attacks by integrating current and CB status monitoring into the group setting adjustment process.

6. Conclusion

In overall, this study has explored the resilience of traditional and adaptive OCR protection schemes in the face of various cyber-physical threats within a hybrid smart grid (CIGRE distribution network) framework. Through the investigation, we have demonstrated the effectiveness of the proposed novel adaptive protection scheme based on the real-time monitoring of current values and circuit breaker statuses to enhance OCR coordination and response. This work has showed significant contributions, including the development and implementation of novel adaptive protection schemes grounded in real-time adaptive

methodologies with validation and implementation carried out using the OCR and established programming IEC 61131–3. Furthermore, the establishment of a real-time cyber-physical system testbed, integrating key components such as the SIEMENS 7SJ62 relay and OMICRON-256 test device, has facilitated comprehensive evaluation of adaptive OCR schemes. Through the examination of the consequences of cyber-attacks on power system operations and adaptive OCR protection schemes, we have highlighted the potential vulnerabilities and the need for robust protection mechanisms. The findings showed the importance of the proposed adaptive OCR approach in supporting power system resilience against cyber-physical threats.

Funding

This work is supported by funding from the Scientific Research and Innovation Support Fund, Ministry of Higher Education Scientific Research, The Hashemite Kingdom of Jordan, under grant number (ENE/1/02/2022), https://cyberssgridhu.github.io/index.html.

CRediT authorship contribution statement

Feras Alasali: Writing – review & editing, Writing – original draft, Supervision, Software, Methodology, Investigation, Funding acquisition, Formal analysis, Conceptualization. **Naser El-Naily:** Writing – original draft, Validation, Software, Methodology, Investigation, Formal analysis, Data curation. **William Holderbaum:** Writing – review & editing, Visualization, Validation, Supervision, Software, Methodology. **Haytham Y. Mustafa:** Writing – review & editing, Visualization, Validation, Supervision, Software, Project administration, Methodology. **Anas AlMajali:** Writing – review & editing, Visualization, Supervision, Software, Methodology, Investigation, Conceptualization. **Awni Itradat:** Writing – review & editing, Visualization, Validation, Supervision, Software, Investigation.

Declaration of Competing Interest

We confirm that this work is original and has not been published elsewhere, nor is it currently under consideration for publication elsewhere and the authors declare no conflict of interest. We also confirm that all authors have participated in drafting the article or revising it critically for important intellectual content; approval of the final version.

Data Availability

Data will be made available on request.

Acknowledgment

We would like to thank The Hashemite University (Renewable Energy Center).

Authorship statement

All persons who meet authorship criteria are listed as authors, and all authors certify that they have participated sufficiently in the work to take public responsibility for the content, including participation in the concept, design, analysis, writing, or revision of the manuscript. Furthermore, each author certifies that this material or similar material has not been and will not be submitted to or published in any other publication before its appearance in Energy Reports.

References

Abdelrahman, M.S., Kharchouf, I., Nguyen, T.L., Mohammed, O.A., 2023. A hybrid physical co-simulation smart grid testbed for testing and impact analysis of cyber-attacks on power systems: framework and attack scenarios (Nov.). Energies vol. 16 (23), 7771. https://doi.org/10.3390/en16237771.

Adhikari, U., Morris, T.H., Pan, S., 2014. A cyber-physical power system test bed for intrusion detection systems. In: IEEE PES general meeting-conference &exposition, 2014. IEEE, pp. 1–5.

Adhikari, U., Morris, T.H., Dahal, N., Pan, S., King, R.L., Younan, N.H., et al., 2012. Development of power system test bed for data mining of synchrophasors data, cyber-attack and relay testing in rtds. In: In: IEEE power and energy society general meeting, 2012. IEEE, pp. 1–7.

Alam, M.N., 2019. Adaptive protection coordination scheme using numerical directional overcurrent relays. IEEE Trans. Ind. Inf. vol. 15 (1), 64–73. https://doi.org/10.1109/TII.2018.2834474.

Alam, M.N., Chakrabarti, S., Pradhan, A.K., 2022. Protection of Networked Microgrids Using Relays With Multiple Setting Groups. IEEE Trans. Ind. Inf. vol. 18 (6), 3713–3723. https://doi.org/10.1109/TII.2021.3120151.

Alasali, F., et al., 2024b. The recent development of protection coordination schemes based on inverse of AC microgrid: a review. IET Gener. Transm. Distrib. vol. 18 (1), 1–23. https://doi.org/10.1049/gtd2.13074.

Alasali, F., et al., 2024a. Enhancing resilience of advanced power protection systems in smart grids against cyber–physical threats. IET Renew. Power Gener. vol. 18 (5), 837–862. https://doi.org/10.1049/rpg2.12957.

Alasali, F., El-Naily, N., Zarour, E., Saad, S.M., 2021a. Highly sensitive and fast microgrid protection using optimal coordination scheme and nonstandard tripping characteristics (Jun.). Int. J. Electr. Power Energy Syst. vol. 128, 106756. https://doi.org/10.1016/J.IJEPES.2020.106756.

Alasali, F., El-Naily, N., Zarour, E., Saad, S.M., 2021b. Highly sensitive and fast microgrid protection using optimal coordination scheme and nonstandard tripping characteristics (Jun.). Int. J. Electr. Power Energy Syst. vol. 128, 106756. https://doi.org/10.1016/J.IJEPES.2020.106756.

Alvarez de Sotomayor, A., Della Giustina, D., Massa, G., Dedè, A., Ramos, F., Barbato, A., 2018. IEC 61850-based adaptive protection system for the MV distribution smart grid (Sep.). Sustain. Energy Grids Netw. vol. 15, 26–33. https://doi.org/10.1016/J.SEGAN.2017.09.003.

Amin, B.M.R., Taghizadeh, S., Rahman, Md.S., Hossain, Md.J., Varadharajan, V., Chen, Z., 2020. Cyber attacks in smart grid – dynamic impacts, analyses and recommendations. IET Cyber-Phys. Syst.: Theory Appl. vol. 5 (4), 321–329. https://doi.org/10.1049/iet-cps.2019.0103.

Ataei, M.A., Gitizadeh, M., 2022. A distributed adaptive protection scheme based on multi-agent system for distribution networks in the presence of distributed generations. IET Gener., Transm. Distrib. vol. 16 (8), 1521–1540. https://doi.org/10.1049/gtd2.12351.

Bisheh, H., Fani, B., Shahgholian, G., Sadeghkhani, I., Guerrero, J.M., 2023. An adaptive fuse-saving protection scheme for active distribution networks (Jan.). Int. J. Electr. Power Energy Syst. vol. 144, 108625. https://doi.org/10.1016/J.IJEPES.2022.108625.

Cavalieri, S., Salafia, M.G., 2020. Asset Administration Shell for PLC Representation Based on IEC 61131–3. IEEE Access vol. 8, 142606–142621. https://doi.org/10.1109/ACCESS.2020.3013890.

Dennis Holstein and Cease, 2010. The Impact of Implementing Cyber Security Requirements using IEC 61850 (Aug.). Electra (1286–1146), 1–83 (Aug.).

Dorosti, P., Moazzami, M., Fani, B., Siano, P., 2022. An adaptive protection coordination scheme for microgrids with optimum PV resources (Mar.). J. Clean. Prod. vol. 340, 130723. https://doi.org/10.1016/J.JCLEPRO.2022.130723.

El-Hamrawy, A.H., 2022. Improved Adaptive Protection Scheme Based Combined Centralized/Decentralized Communications for Power Systems Equipped With Distributed Generation. IEEE Access vol. 10, 97061–97074.

El-Naily, N., Saad, S.M., Elhaffar, A., Zarour, E., Alasali, F., 2022. Innovative adaptive protection approach to maximize the security and performance of phase/earth overcurrent relay for microgrid considering earth fault scenarios (May). Electr. Power Syst. Res. vol. 206, 107844. https://doi.org/10.1016/J.EPSR.2022.107844.

Elrawy, M.F., Hadjidemetriou, L., Laoudias, C., Michael, M.K., 2023. Modelling and analysing security threats targeting protective relay operations in digital substations. 2023 IEEE Int. Conf. Cyber Secur. Resil. (CSR) 523–529. https://doi.org/10.1109/CSR57506.2023.10224964.

Fu, X., Li, S., Fairbank, M., Wunsch, D.C., Alonso, E., 2015. Training recurrent neural networks with the Levenberg–Marquardt algorithm for optimal control of a grid-connected converter. IEEE Trans. Neural Netw. Learn Syst. 26 (9), 1900–1912.

Ghalei Monfared Zanjani, M., Mazlumi, K., Kamwa, I., 2018. Application of μPMUs for adaptive protection of overcurrent relays in microgrids. IET Gener. Transm. Distrib. vol. 12 (18), 4061–4068. https://doi.org/10.1049/iet-gtd.2018.5898.

Gutierrez-Rojas, D., Demidov, I., Kontou, A., Lagos, D., Sahoo, S., Nardelli, P.J., 2023. Operational issues on adaptive protection of microgrids due to cyber attacks. IEEE Trans. Circuits Syst. II: Express Briefs vol. 70 (8), 2994–2998. https://doi.org/10.1109/TCSII.2023.3245664.

Habib, H.F., Hariri, M.El, Elsayed, A., Mohammed, O.A., 2018b. Utilization of supercapacitors in protection schemes for resiliency against communication outages: a case study on size and cost optimization. IEEE Trans. Ind. Appl. vol. 54 (4), 3153–3164. https://doi.org/10.1109/TIA.2018.2819620.

Habib, H.F., Hariri, A.O., ElSayed, A., Mohammed, O.A., 2017b. Deployment of electric vehicles in an adaptive protection technique for riding through cyber attack threats in microgrids. 2017 IEEE Int. Conf. Environ. Electr. Eng. 2017 IEEE Ind. Commer. Power Syst. Eur. (EEEIC / ICPS Eur.) 1–6. https://doi.org/10.1109/EEEIC.2017.7977729.

Habib, H.F., Lashway, C.R., Mohammed, O.A., 2018a. A Review of Communication Failure Impacts on Adaptive Microgrid Protection Schemes and the Use of Energy

Storage as a Contingency. IEEE Trans. Ind. Appl. vol. 54 (2), 1194–1207. https://doi.org/10.1109/TIA.2017.2776858.
Habib, H.F., Mohamed, A.A.S., El Hariri, M., Mohammed, O.A., 2017a. Utilizing supercapacitors for resiliency enhancements and adaptive microgrid protection against communication failures (Apr.). Electr. Power Syst. Res. vol. 145, 223–233. https://doi.org/10.1016/J.EPSR.2016.12.027.
Hansen, A., Staggs, J., Shenoi, S., 2017. Security analysis of an advanced metering infrastructure (Sep.). Int. J. Crit. Infrastruct. Prot. vol. 18, 3–19. https://doi.org/10.1016/J.IJCIP.2017.03.004.
Ibtissam, K., Abdelrahman, M.S., Alrashide, A., Mohammed, O.A., 2022. Assessment of protection schemes and their security under denial of service attacks. 2022 IEEE Int. Conf. Environ. Electr. Eng. 2022 IEEE Ind. Commer. Power Syst. Eur. (EEEIC / ICPS Eur.) 1–6. https://doi.org/10.1109/EEEIC/ICPSEurope54979.2022.9854745.
Jahromi, A.A., Kemmeugne, A., Kundur, D., Haddadi, A., 2020. Cyber-physical attacks targeting communication-assisted protection schemes. IEEE Trans. Power Syst. vol. 35 (1), 440–450. https://doi.org/10.1109/TPWRS.2019.2924441.
K. A, V. C, 2024. Design of adaptive protection coordination scheme using SVM for an AC microgrid (Jun.). Energy Rep. vol. 11, 4688–4712. https://doi.org/10.1016/J.EGYR.2024.04.021.
Karimipour, N., Arani, M.F.M., Jahromi, A.A., 2023. Cyberattack threats against adaptive protection systems in microgrids. 2023 IEEE Power Energy Soc. Gen. Meet. (PESGM) 1–5. https://doi.org/10.1109/PESGM52003.2023.10252747.
Kasap, H., Purlu, M., Turkay, B.E., Ganjavi, R., 2023. Tap staggering analysis and effects on the adaptive protection system in networks with renewable energy sources. IEEE Access vol. 11, 138623–138637. https://doi.org/10.1109/ACCESS.2023.3339782.
Liu, S., Chen, B., Zourntos, T., Kundur, D., Butler-Purry, K., 2014. A coordinated multi-switch attack for cascading failures in smart grid. IEEE Trans. Smart Grid vol. 5 (3), 1183–1195. https://doi.org/10.1109/TSG.2014.2302476.
Mallouhi, M., Al-Nashif, Y., Cox, D., T. Chadaga, S.A., 2011. Hariri Testbed for Analyzing Security of Scada Control Systems (tasscs). 2011 IEEE PES innovative smart grid technologies (ISGT). IEEE, pp. 1–7.
M. McDonald, J. Mulder, B. Richardson, R. Cassidy, A. Chavez, N. Pattengale, et al. Modeling and simulation for cyber-physical system security research, development and applications, Sandia National Laboratories. Tech. Rep. Sandia Report SAND2010-0568.
Memon, A.A., Kauhaniemi, K., 2021. Real-time hardware-in-the-loop testing of IEC 61850 GOOSE-based logically selective adaptive protection of AC microgrid. IEEE Access vol. 9, 154612–154639. https://doi.org/10.1109/ACCESS.2021.3128370.
Mohamed, A.S., Kundur, D., Khalaf, M., 2024. A probabilistic approach to adaptive protection in the smart grid (Apr.). ACM Trans. Cyber-Phys. Syst.. https://doi.org/10.1145/3656347.
Molina, D., Venayagamoorthy, G.K., Liang, J., Harley, R.G., 2013. Intelligent local area signals based damping of power system oscillations using virtual generators and approximate dynamic programming. IEEE Trans. Smart Grid 4 (1), 498–508.
Mukherjee, D., 2022. Data-driven false data injection attack: a low-rank approach. IEEE Trans. Smart Grid vol. 13 (3), 2479–2482. https://doi.org/10.1109/TSG.2022.3145633.
National SCADA Testbed Program. Idaho National Laboratory, ⟨https://www.inl.gov/⟩.
Núñez-Mata, O., Palma-Behnke, R., Valencia, F., Mendoza-Araya, P., Jiménez-Estévez, G., 2018. Adaptive protection system for microgrids based on a robust optimization strategy (Feb.). Energies vol. 11 (2), 308. https://doi.org/10.3390/en11020308.
Núñez-Mata, O., Palma-Behnke, R., Valencia, F., Urrutia-Molina, A., Mendoza-Araya, P., Jiménez-Estévez, G., 2019. Coupling an adaptive protection system with an energy management system for microgrids (Dec.). Electr. J. vol. 32 (10), 106675. https://doi.org/10.1016/J.TEJ.2019.106675.
Papaspiliotopoulos, V.A., Korres, G.N., Kleftakis, V.A., Hatziargyriou, N.D., 2017. Hardware-In-the-Loop Design and Optimal Setting of Adaptive Protection Schemes for Distribution Systems With Distributed Generation. IEEE Trans. Power Deliv. vol. 32 (1), 393–400. https://doi.org/10.1109/TPWRD.2015.2509784.
Pola, S., Jovanovic, M., Azzouz, M., Mirhassani, M., 2023. Cyber resiliency enhancement of overcurrent relays in distribution systems. IEEE Trans. Smart Grid (p. 1). https://doi.org/10.1109/TSG.2023.3344632.
Poudel, S., Ni, Z., Malla, N., 2017. Real-time cyber physical system testbed for power system security and control. Electr. Power Energy Syst. 90, 124–133.
Rahmati, A., Dimassi, M.A., Adhami, R., Bumblauskas, D., 2015. An Overcurrent Protection Relay Based on Local Measurements (May). IEEE Trans. Ind. Appl. vol. 51 (3), 2081–2085. https://doi.org/10.1109/TIA.2014.2385933.
Sampaio, F.C., Leão, R.P.S., Sampaio, R.F., Melo, L.S., Barroso, G.C., 2020. A multi-agent-based integrated self-healing and adaptive protection system for power distribution systems with distributed generation (Nov.). Electr. Power Syst. Res. vol. 188, 106525. https://doi.org/10.1016/J.EPSR.2020.106525.
Shih, M.Y., Conde, A., Leonowicz, Z., Martirano, L., 2017. An adaptive overcurrent coordination scheme to improve relay sensitivity and overcome drawbacks due to distributed generation in smart grids. IEEE Trans. Ind. Appl. vol. 53 (6), 5217–5228. https://doi.org/10.1109/TIA.2017.2717880.
Xiong, J., Zhu, G., Huang, Y., Shi, J., 2020. A user-friendly verification approach for IEC 61131-3 PLC programs (Mar.). Electronics vol. 9 (4), 572. https://doi.org/10.3390/electronics9040572.
Yousefi kia, M., Saniei, M., Seifossadat, S.G., 2023. A novel cyber-attack modelling and detection in overcurrent protection relays based on wavelet signature analysis. IET Gener., Transm. Distrib. vol. 17 (7), 1585–1600. https://doi.org/10.1049/gtd2.12766.