Hierarchically Coordinated Protection: A Key Element in Improving Power System Resilience

Mohammad Tasdighi, *Student Member, IEEE* and Mladen Kezunovic, *Life Fellow, IEEE*
Department of Electrical Engineering
Texas A&M University
College Station, United States of America
m.tasdighi@tamu.edu, kezunov@ece.tamu.edu

***Abstract*—This paper investigates the challenges of conventional transmission protection system dependability and security when meeting the operating complexities affecting power system resilience. Effective Hierarchically Coordinated Protection (HCP) scheme is proposed to illustrate various approaches to corrective, adaptive and predictive protection actions aimed at improving power system resilience. The results obtained using IEEE test cases are used to illustrate the benefits.**

Keywords—Hierarchically coordinated protection; evolving network topology; unintended DG tripping; wide area measurements; machine learning algorithms

I. Introduction

A. Power System Resilience

Due to increase in today's power system complexity, it is becoming more obvious that the classical reliability-based perspective alone would not be sufficient in assuring a continuous power supply [1]. The emerging economic and environmental concerns have resulted in introduction of renewables, distributed generation, microgrids and other electricity grid infrastructure changes creating operating uncertainties. Therefore, it is required from the power system to be resilient against the high-impact low-probability events, as well as conventional threats, and hence to surpass the existing performance [1].

There is not a universally accepted definition for the concept of resilience as it has been defined in several ways. According to the UK Energy Research Center [2], resilience is defined as "the capacity of an energy system to tolerate disturbance and to continue to deliver affordable energy services to consumers. A resilient energy system can speedily recover from shocks and can provide alternative means of satisfying energy service needs in the event of changed external circumstances." Reference [3] defines a resilient system as a system which degrades gradually, and not abruptly, when it experiences stressed conditions and it is able to restore back into its normal state thereafter. The National Infrastructure Advisory Council (NIAC), USA [4], adds another property to the resilient system definition where a resilient system learns from its previous lessons and experiences under major disturbances and uses this knowledge to adapt and fortify itself to prevent or mitigate the consequences of a similar event in the future. The Cabinet Office U.K. defines a resilient system as a system able to ". . .anticipate, absorb, adapt to and/or rapidly recover from a disruptive event" [5]. Resilience is defined in [6] as the "robustness and recovery characteristics of utility infrastructure and operations, which avoid or minimize interruptions of service during an extraordinary and hazardous event". The US National Academies report considers a resilient system the one which plans and prepares for a disruptive event, absorbs it and can recover from it. More importantly, it adapts itself for similar future events [7].

Unlike reliability, which is a static concept, resilience has a dynamic, unfolding, and time-variant nature. The main features of resilience are robustness (withstand low probability but high consequence events), resourcefulness (effectively manage a disturbance as it unfolds), rapid recovery (get things back to normal as fast as possible after the disturbance), and adaptability (absorb new lessons from a catastrophe).

Various aspects of power system such protection, operation, planning, etc. should function hand in hand properly to improve system's resilience. The focus of this paper is to investigate how the protection reliability affects resiliency.

B. The Impact of Protection Reliability on Resiliency

Our view of protection system reliability focuses on dependability and security [8]. A protection system operating correctly in the case of faults within its protection zone is defined as being dependable [9]. The security, on the other hand, focuses on preventing the protection system's incorrect operation for faults out of protected zone or for normal (no-fault) operating conditions [10].

After an extensive study of the major disturbances and blackouts in the recent history, it has been concluded that frequently they have been associated with both dependability and security based protection system failures [11]. Relay misoperation is known to be a contributing factor in 75 percent of the major disturbances in North America [11]. During abnormal conditions, the backup relays sometimes cannot differentiate faults from no-fault conditions, such as when overload and large power swings occur. It has been noted that while redundancy reduces, the probability of a dependability-based protection system failure, it may increase the probability of a security based protection system failure [8,11]. As a result, the balance between dependability and security of protective relay operation remains a challenge. An improved protection system designs must provide inherently dependable and secure operation. The hierarchically coordinated protection (HCP) approach aims at achieving that goal.

The rest of the paper is organized as follows: Section II gives a brief background on system resilience and the role of protection security and dependability in improving it. It also reviews the new concept of HCP. Section III introduces new challenges that the conventional protection schemes are facing and offers hypothesis for the solutions. Section IV presents the proposed solutions and methodologies. Results of test cases are discussed in Section V. The concluding remarks are summarized in Section VI. References are given at the end.

978-1-5386-3669-5/18/$31.00 ©2018 IEEE

II. BACKGROUND

Following a disturbance, the system may experience a transition between various operating states based on the severity of the disturbance [1]. Figure 1 shows the change of the resilience on a resilience curve as the system transitions between the various states unfold. When the system is operating at normal state, i.e. operational constraints as well as security margins are satisfied and respected. The system is robust enough to handle a single (N-1) disturbance effectively. Following the disturbance, resiliency degrades depending on the severity of the disturbance and the system enters the post-event state. Resourcefulness, redundancy, and adaptive self-organizing can play a critical role at this state to provide opportunities for implementing corrective, preventive, emergency, or in extreme mitigating actions to minimize the degradation level (R_o−R_{pe}) before restoration process begins. Finally, after the disturbance resulted in an outage, the restorative actions should be taken to restore the system into normal conditions and recover its highest resiliency.

To better clarify the impact of protection reliability on system's resilience, we can compare the legacy protection reliability-based perspective with the requirements asked for resilience today. While the legacy protection on transmission may be able to handle the N-1 contingency case without causing any misoperation, it may not be able to cope with N-m contingency cases effectively. In other words, static predetermined balance between dependability and security might not meet the system's resilience criteria necessarily. As Fig. 1 shows, the system's resilience is characterized by resiliency level at various states of the system as well as the transition time between the states. Maintaining the balance between protection dependability and security improves the gradual degradation by minimizing resilience degradation level (R_o−R_{pe}), as well as increasing degradation time (t_{pe}−t_e) as the system experiences N-m contingencies.

A dynamic trade-off between security and dependability is needed as the system goes through events. HCP concept has been recently proposed in response to a need for dynamic trade-off between protection security and dependability [12-13]. Figure 2 shows HCP that supervises traditional distance relay function for transmission lines. The basic idea behind this concept is a dynamic balance between dependability and security, which is obtained through predictive, adaptive and corrective protection actions. This provides flexibility in the protection schemes behavior to handle the uncertainties associated with the protection operation. [12-13]. The three layers of protection (predictive, adaptive, and corrective), is aimed at balancing the dependability vs security dynamically to prepare for the disruptive events, absorb them, and recover from them with an appropriated relaying action.

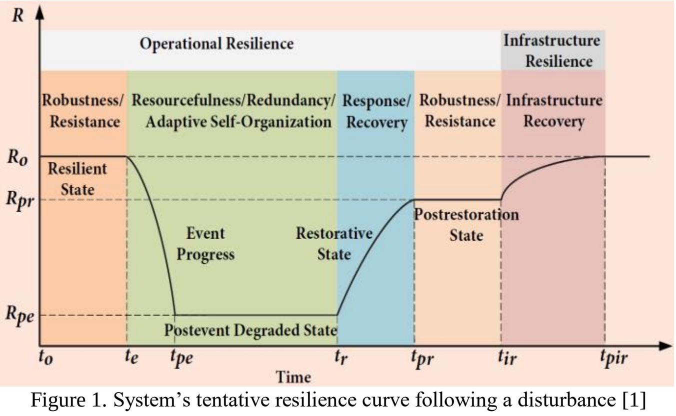

Figure 1. System's tentative resilience curve following a disturbance [1]

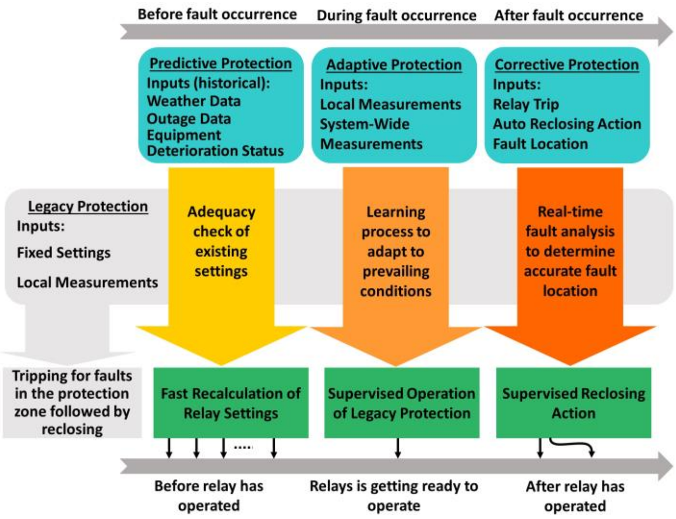

Figure 2. Legacy distance protection supervised by HCP

Historical data and statistics on previous contingencies such as weather-related disturbances, equipment outages, etc. is employed by the Predictive Protection layer to identify similar conditions which may lead to the major disturbances in the future. Possible anticipation of disturbance by this layer provides an opportunity of adjusting bias between dependability and security for the protection system by selecting between groups of relay settings as an example.

Inherently Adaptive Protection layer, which is based on the learning algorithms from patterns of the features extracted from the real-time system measurements comes next. Numerous system conditions are involved in the learning process to cover the potential scenarios and then the pattern from real-time measurements are compared against those for system's condition identification. This allows maintaining protection dependability and security without the need to outweigh one against the other.

The corrective layer deals with assessing the correctness of the protection system operation in real time by utilizing a tool to detect relay misoperation. Should a legacy protection scheme operate, this tool is activated immediately after to detect any misoperation and the corrective action because of that misoperation is initiated as needed.

Such protection adjustment approaches may be coordinated in a hierarchical way by implementing the predictive, adaptive and corrective actions simultaneously to assure improved resiliency by avoiding various unwanted relay operations.

III. PROBLEM DESCRIPTION

Increased system complexities aimed at alleviating the grid operating difficulties could impede proper functioning of conventional protection schemes and make maintaining protection reliability more difficult, which in turn may hurt the system's resilience. To facilitate implementing these complexities in today's power systems' operation, the challenges of maintaining proper operation of conventional protection schemes and how to resolve them should be investigated. The complexities under consideration in this paper are: 1) more frequent network topology changes because of switching actions, 2) high penetration of DGs (renewables specifically) into power systems, and 3) required sensitive anti-islanding controls and measures on DG interconnections.

A. *Evolving Network Topology*

Multiple switching actions for various objectives such as avoiding congestion and mitigating cascades, preventing load-shedding, reducing the operation cost, supporting maintenance purposes, etc. is a big operational change which is gaining much attention these days [14]. However, it also could be considered as one of the major causes of deterioration of reliability of the conventional protection operation [15]. Evolving network topology may cause a change in the network short circuit value and affect setting coordination of the distance relays consequently [15]. The network relay settings that are set for a base network topology, might not be adequate for an evolving topology and the protection reliability might get affected. Revisiting the setting coordination adequacy for evolving network topology seems to be critical in assuring that such an operating complexity does not affect resiliency.

B. High Penetration of Renewables

It has been recognized that employing renewables as new sources of power will be significantly beneficial from both economic and environmental perspectives [16-17]. The new trend is towards incorporating significant amounts of renewables into power systems [16-17]. However, it is still a challenge to realize how to deal with their uncertain generation and its consequences on the power system resilient operation. As an example, from the transmission protection point of view, the uncertain power generation by renewables is translated into varying power flows on the lines that in case of significant changes could become a threat to proper operation of distance relay backup zones with respect to their loading limits. Currently, the distance relays are set in a network assuming that the loading of the lines are known to a certain extent [18]. The transmission protection schemes should be able to predict the protection vulnerabilities because of major power flow changes to maintain the protection dependability and security.

C. Anti-Islanding Protection Measures

Microgrid technology and decentralized energy systems with the large-scale deployment of distributed energy resources and decentralized control can play a key role in providing resilience against system disturbances [1]. However, the standards for DG interconnection protection and control measures for detaching DGs from the grid under certain circumstances might act as a threat to upstream protection coordination as DG penetration increases in the system [16-17]. NERC has recently reported an unintended tripping of 1200 MW PV generation from the grid because of sensitive under frequency/voltage protection measures on the interconnection point [19]. The sudden power flow increase to compensate the lack of DG in the system which is already under stress of previous disturbance as well as probable loss of synchronism between generators could initiate distance relay misoperation and lead to cascade events [20].

IV. Examples of Proposed Methodologies

A. Predictive Protection

Following a network topology change or before it happens (if planned or predicted), it is critical to identify which relay settings are/will be affected. Having an estimate of how far, in terms of electrical distance, from the place of topology change one can expect the relay settings to get affected is of significant value in predicting vulnerable relay settings for an evolving topology. This concept is called distance of impact (DoI) [15] an example of which is shown in Fig. 3. DoI of one from the switched transmission line a-b, includes the buses c to f with their corresponding branches and relays, and DoI of two includes those of the buses c to j. DoI concept can be verified by conducting numerous simulations on the test systems as

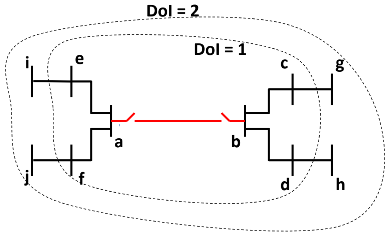

Figure 3. Illustrating the concept of DoI

discussed in the next Section. Using the DoI measure, the focus of concern is narrowed down to a certain number of relays for their existing settings adequacy check. This saves significant computation burden as well. Then, fast setting calculation techniques using advanced computational technology can be employed to propose the best set of settings for those relays under an evolving topology.

An automated real-time distance relay settings coordination adequacy check module is proposed which considers the current/future network topology as well as loading of the lines and identifies the vulnerable relays in real-time. Such module can be implemented at the control center level for continuous monitoring and vulnerability analysis. It can also be connected to the substation level to closely monitor the vulnerable relays. Predicting settings inadequacy in the system provides a better view and understanding on the consequences of contingencies and how they may unfold.

Figure 4 shows the general flowchart of the proposed module. Parallel computation is utilized in calculation of fault databases, highlighted blocks in Fig. 4, to improve the calculation speed. Each database contains the values of network's bus voltages and branch currents for the corresponding type of fault to be used for apparent impedances calculations. To be able to implement parallel computation on multiple tasks, they should be independent from each other. In other words, the tasks should not need a flow of data between them to be performed. The phase distance setting calculation procedure, equations required for updating the three highlighted blocks in Fig. 4, fit the above mentioned parallel computation criteria. Further details may be found in [15].

B. Adaptive Protection

An example of unintended DG tripping impact on conventional distance protection security is shown in Fig. 5 for a test relay on New-England 39-bus system. A fault

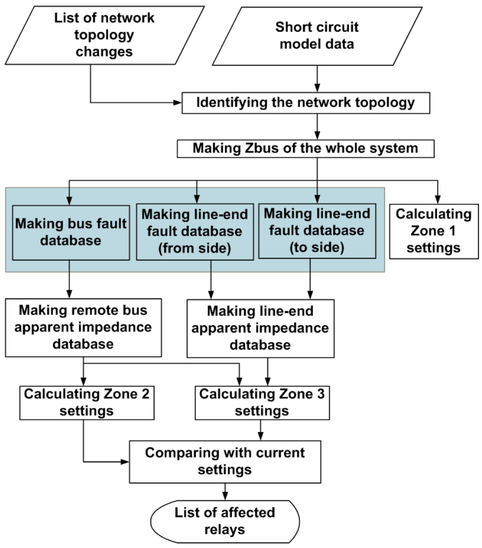

Figure 4. General flowchart of the settings calculation module

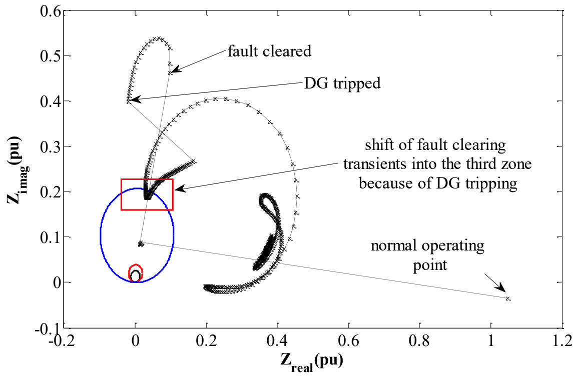

Figure 5. DG tripping impact on apparent impedance trajectory

happening/clearing action on the system is accompanied by a DG tripping event on a neighboring area; this is a simulated test case for a target relay as will be discussed more in the next Section. Because of this event, the impedance trajectory seen by the relay is pushed into its backup third zone which may lead to relay misoperation. Hence, the transmission side should be facilitated with adaptive protection schemes to maintain the protection reliability under such completely unpredictable events. For this matter, machine-learning algorithms can be employed to allow relays to recognize such critical events from faults and adapt their operation to the prevailing conditions.

The candidate relays which are vulnerable to unintended DG tripping events in a system can be identified using previously discussed setting adequacy check module. At the substation level, a Support Vector Machine (SVM) based protection scheme, shown in Fig. 6, is proposed. It can be trained to capture the interactions of system's dynamic behavior with distance backup protective zones because of DG tripping and enable the candidate relays to distinguish between a fault and such an event. The tripping logic is based on the classification of the input features extracted from the system measurements. The classification criteria are learned by SVM when being trained by numerous input features from potential faults and DG tripping events in the system. This way the unexpected interferences with distance relays' protective zones can be supervised to achieve a balance between protection dependability and security consequently.

SVM-1 and SVM-2, shown in Fig. 6, are multiclass SVMs which are trained based on local data only and wide area (WA) data in addition to local data respectively. The accuracy is improved when using the WA measurements as will be illustrated in next Section. Class labels are assigned as "1 = faults", "0 = DG tripping", and "-1 = other". Cases in class "1" are filtered by the comparator as they are not of interest and the logical AND of the comparator output and the pickup signal of distance backup zones identifies the trip/block signal.

Bus voltage phasor, line current phasor magnitude, line active and reactive power flow, which are represented by V_{bus}, $|I_{line}|$, P_{line}, and Q_{line} respectively, are the local features selected as inputs for both SVMs. The active (P_{DG}) and reactive power (Q_{DG}) injected to the grid from the PCC as well as the voltage phasor at the PCC (V_{DG}) are the features selected from WA measurements utilized to train SVM-2. Further details may be found in [16]. It should be noted that the WA measurements can be obtained from either PMUs or digital distance relays. No optimal PMU placement is deployed here; the measurements required are from the PCC, the target relay, and a reference bus to achieve relative phasor angles which are timely synchronized.

C. Corrective Protection

Distance relays may misoperate by seeing a fault in a protective zone by mistake when the fault is in another zone or out of zones of the relay; a no-fault condition seen as a fault within a protective zone of the relay, e.g. power swings, etc. When a relay operates, an on-line fault analysis can identify its correct/incorrect operation by detecting and locating the fault. If this analysis is performed with a sufficiently high speed, it can be employed in supervising conventional reclosing scheme to correct a misoperation of the relay.

In a previous research effort [21], a fault detection and location technique based on fast synchronized sampling with high accuracy as well as event tree methods were employed to implement a relay misoperation detection tool at the substation level. Having a transmission line tripped, the tool is activated to verify the operation correctness of the relay and in case of detecting any misoperation, the line can be put back into service quickly. Very high speed of fault analysis has been achieved by the proposed method such that it could be deployed to impact the reclosing applications [21]. A transmission line which is facilitated with event-triggered measurements (digital fault recorders (DFRs)) from its two ends is shown in Fig. 7. Different intelligent electronic devices (IEDs) at the substation can monitor the line at both ends, as shown for one end in Fig. 7. Any event seen as a fault by the digital protective relay (DPR) triggers IEDs to capture the event measurements. Thanks to Global Positioning System (GPS) technology, synchronized and time-stamped data

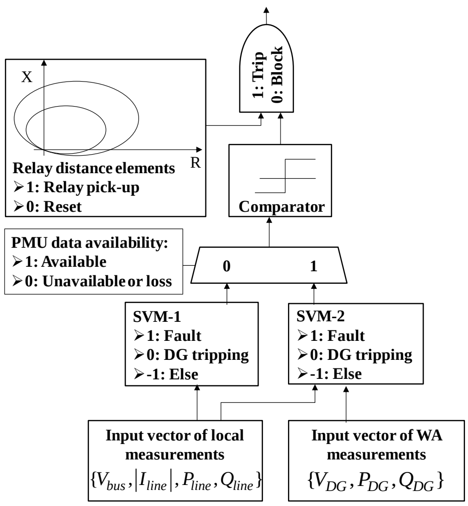

Figure 6. Block diagram of the proposed scheme

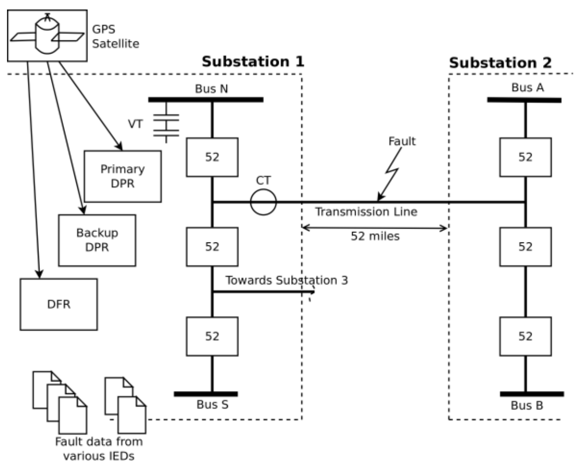

Figure 7. Transmission line setup with measurements from both ends

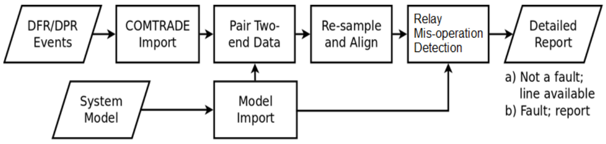

Figure 8. Automated analysis of time-synchronized event data

samples are available using high-speed communication link between substations and control center. Figure 8 shows the general flowchart of the proposed relay misoperation detection tool. Further details may be found in [13, 21].

V. Case Studies and Results

A. *Identifying Vulnerable Relays in the System*

Various test systems are utilized to assess the performance of the proposed setting calculation module. Commercial CAPE software is utilized as a benchmark to verify the results [22]. Alberta transmission operator system with ~2500 buses and ~3000 branches is chosen to evaluate the performance of the module on real-life scale systems. 1000 random N-2 contingency cases, assuming two lines switched out, from all over the network are chosen to conduct a sensitivity analysis. Top 10 critical cases with maximum number of relays experiencing settings inadequacy are shown in Table I.

It was concluded that for all the 1000 cases, DoI never extends beyond 5 on this system. DoI helps reducing computation burden significantly as the associated calculations to identify the affected relay settings are needed to be performed on a smaller part of the network. The computation time for performing the cases in Table I when implementing DoI and without implementing it is shown in Fig. 9. Utilizing 30 processing nodes from supercomputing facility [23] as well as MATLAB, parallel computation has been implemented in all cases. It is worth noting that conducting each case without implementing parallel computation and DoI was observed to be ~ 40000 seconds.

B. *SVM-Based Classification*

This part of the study has been tested on New England 39 bus system. The required input data for training and testing processes of SVMs is obtained from numerous simulations on the test system. Simulations have been performed by PSS/E software on a PC with an Intel Xeon W3530 C 2.8 GHz CPU. Bus 27 is considered as DG PCC, Fig. 10. The previously developed relay setting adequacy check module is utilized on the system to identify the candidate relays prone to misoperate under unintended DG tripping events. The results rank $R_{25\text{-}26}$, $R_{29\text{-}26}$, and $R_{16\text{-}17}$ as the top three vulnerable relays. The proposed SVM-based scheme is implemented for Relay $R_{25\text{-}26}$ as the most critical relay.

Different capacities assumed for the tripped DGs in the system, different fault locations around the PCC, and various

Table I. N-2 Contingency cases affecting major relay settings

Rank	Lines (from-to)	NoAR*	DoI
1	89-91 & 579-585	29	5
2	420-865 & 666-1691	29	5
3	420-865 & 1318-1344	25	5
4	207-590 & 666-1200	23	3
5	208-581 & 242-253	23	4
6	35-331 & 167-737	22	5
7	297-483 & 669-677	22	5
8	35-331 & 666-1670	22	5
9	152-988 & 1431-1484	22	4
10	63-821 & 136-514	21	4

* Number of Affected Relays

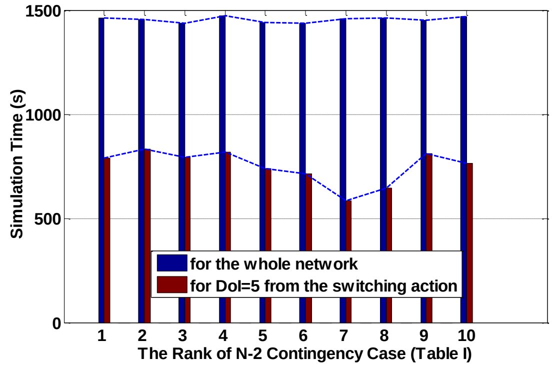

Figure 9. Simulation time with and without implementing DoI

DG tripping instants following the fault are assumed to include several scenarios for creating SVMs training and testing data sets. The classification accuracy results for two SVMs is summarized in Table II. As it shows, the classification accuracy using WA measurements is improved. Employing local measurements only, also results in an acceptable level of accuracy. A testing scenario, shown in Fig. 11, is chosen to compare the performance of the proposed method for any of the two SVMs with that of the conventional relay pickup. A three-phase fault on the middle of the line 26-29 at t = 1s is cleared 0.2s later by tripping the line out. An unintentional DG tripping event, 250 MW PV, happens at t = 1.65s following the fault clearing event. To assess the dependability of the proposed method under system's complex and stressed conditions, another fault is simulated at t = 2.5s on the line 26-28, when the system is still dealing with previous stresses, to see if it is detected by the proposed method. As Figure 11 shows, the distance element of the relay picks up on the first fault happening and does not drop while the SVMs have differentiate the fault events from the DG tripping event and properly block/unblock the relay operation. As was expected from previous results, SVM-2 has done a better classification especially in detecting the second fault. As results show, the proposed approach can detect a fault during the blocking period and unblock the relay for a correct operation which is a significant advantage over the currently used blocking schemes (state of the art) to maintain the protection dependability in addition to security.

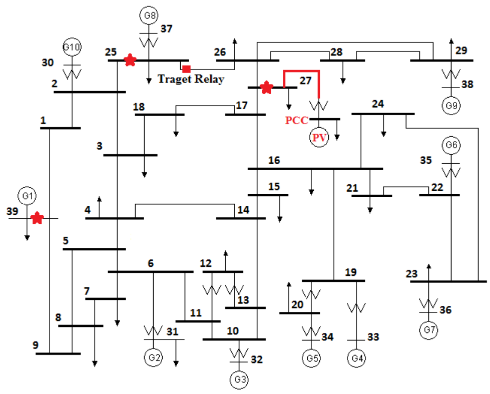

Figure 10. New-England 39 bus system with DG penetration

Table II. SVMs specifications

SVM No.	SVM-1	SVM-2
Testing Accuracy (%)	93.8	97.6
Training Time (s)	39.67	8.76
Testing Time (s)	0.147	0.19

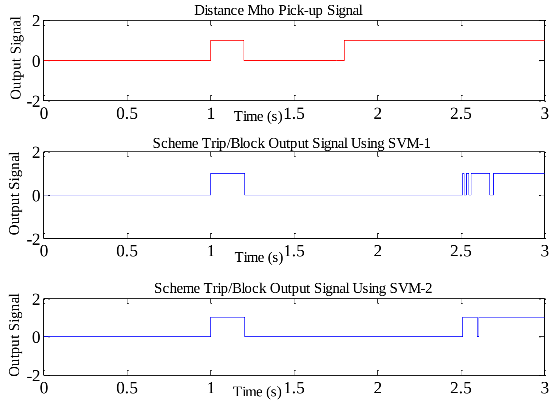

Figure 11. SVM performance comparison

C. Relay Misoperation Detection

Various test cases from simulations and field data are deployed to assess the performance of the relay misoperation detection tool. The following example demonstrates the performance of the tool for a relay misoperation case. Field recordings from actual IEDs have been utilized to provide the sampled data. Fig. 12 shows how the module has detected the relay misoperation. Instantaneous power from both ends of the line, illustrated in Fig. 12 (a-c), is calculated from data captured by DFRs. According to the utility's investigation on this case, the fault happened on a neighboring line and it is concluded that the relay has falsely tripped because of a single line to ground fault on an adjacent line. According to Fig. 12 (a-c), it is observed that the instantaneous powers from both ends stay in opposite direction before and after the fault so the tool interpret this as "no fault" condition. Figure 12 (d-f) shows the sign function (sgn-plot) of three phase power differences from two ends as a function of time which illustrates most of the samples are not zero. This means detection of no fault in any of the phases according to the method's algorithm. Further details might be found in [21].

VI. CONCLUSION

The main contributions of this study are as follows:

- The impact of legacy distance protection on power system resilience has been identified for the cases when distance relaying loses it selectivity.
- A fundamental framework for the HCP-based scheme is proposed to supervise distance protection function and its impact on resiliency by improving protection reliability.
- Examples of novel approaches for predictive, adaptive, and corrective protection, previously proposed by the authors, are combined to illustrate how the HCP-based scheme can provide a dynamic trade-off between protection security and dependability.
- The performance effectiveness of the proposed approaches compared to the legacy distance protection is illustrated using data from a real-life and IEEE test systems.

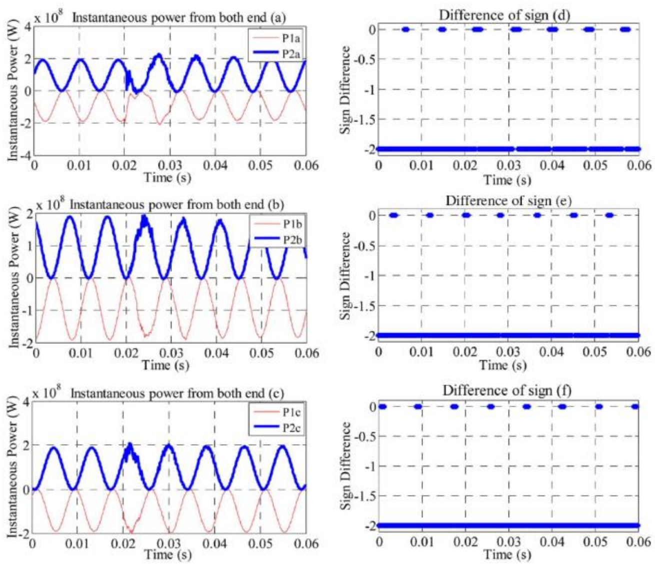

Figure 12. Detection of relay misoperation

REFERENCES

[1] M. Panteli and P. Mancarella, "The Grid: Stronger, Bigger, Smarter?: Presenting a Conceptual Framework of Power System Resilience," in *IEEE Power and Energy Magazine*, vol. 13, no. 3, pp. 58-66, 2015.

[2] M. Chaudry, *et al.*, Building a Resilient UK Energy System. London, U.K.: UK Energy Research Center (UKERC), Apr. 14, 2011.

[3] T. J. Overbye, *et al.*, Engineering Resilient Cyber Physical Systems. Tempe, AZ, USA: PSERC, May 2012, ser. PSERC Publication 12-16.

[4] A Framework for Establishing Critical Infrastructure Resilience Goals, NIAC,Washington, DC, USA, Oct. 2010.

[5] Cabinet Office, "Keeping the country running: Natural hazards and infrastructure," London, U.K., Oct. 2011.

[6] M. Keogh and C. Cody, Resilience in Regulated Utilities. Washington, DC, USA: The National Association of Regulatory Utility Commissioners (NAURC), Nov. 2013.

[7] National Academies of Sciences, Engineering, and Medicine. 2017. Enhancing the Resilience of the Nation's Electricity System. Washington, DC: The National Academies Press.

[8] NERC System Protection and Control Task Force, "Protection System Reliability, Redundancy of Protection System Elements," Nov. 2008

[9] E. A. Udren et al., "Proposed statistical performance measures for microprocessor-based transmission-line protective relays. Part I. Explanation of the statistics," in IEEE Transactions on Power Delivery, vol. 12, no. 1, pp. 134-143, Jan 1997.

[10] E. A. Udren *et al.*, "Proposed Statistical Performance Measures for Microprocessor-Based Transmission-Line Protective Relays, Part 2: Collection and Uses of Data," in *IEEE Power Engineering Review*, vol. 17, no. 1, pp. 43-43, January 1997.

[11] U.S.-Canada Power System Outage Task Force, "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations," Tech. Rep., Apr. 2004.

[12] M. Kezunovic B. Matic Cuka "Hierarchical Coordinated Protection with High Penetration of Smart Grid Renewable Resources (2.3)" PSERC Future Grid Initiative 2013.

[13] M. Kezunovic, *et al.*," Hierarchically Coordinated Protection: An Integrated Concept of Corrective, Predictive, and Inherently Adaptive Protection," CIGRE, Sochi, Russia, June 2015.

[14] K. W. Hedman, S. S. Oren and R. P. O'Neill, "A review of transmission switching and network topology optimization," 2011 IEEE Power and Energy Society General Meeting, San Diego, CA, 2011, pp. 1-7.

[15] M. Tasdighi and M. Kezunovic, "Automated Review of Distance Relay Settings Adequacy After the Network Topology Changes," IEEE Transactions on Power Delivery, no. 4, pp. 1873-1881, Aug. 2016.

[16] M. Tasdighi and M. Kezunovic, " Preventing transmission distance relays maloperation under unintended bulk DG tripping using SVM-based approach," Electric Power Systems Research, Vol. 142, pp. 258-267, 2017.

[17] J. A. Peças Lopes, et al., "Integrating distributed generation into electric power systems: A review of drivers, challenges and opportunities," Elect. Power Syst. Res., vol. 77, no. 9, pp. 1189–1203, Jul. 2007.

[18] D. M. MacGregor, et al., "Automatic relay setting," *J. of Elec. And Elect. Eng.*, vol. 21, no. 3, pp. 169-179, 2002.

[19] NERC, "1200 MW Fault Induced Solar Photovoltaic Resource Interruption Disturbance Report," Tech. Rep., June 2017.

[20] M. Henderson, Impacts of Transmission System Contingencies on Distributed Generation – Overview, ISO New-England DG forecast group meeting, Dec. 2013.

[21] P. Dutta, A. Esmaeilian and M. Kezunovic, "Transmission-Line Fault Analysis Using Synchronized Sampling," in *IEEE Transactions on Power Delivery*, vol. 29, no. 2, pp. 942-950, April 2014.

[22] [Online] http://arpa-e.energy.gov/

[23] [Online] http://sc.tamu.edu