STUDY THE PERFORMANCE OF POWER SYSTEM PROTECTION USING WIDE AREA MONITORING SYSTEMS

Mysa Aparna[1], Rajeshwar Rao Errabelly[2], Sandeep reddy Ganji[3], Rajesh Thota[4], K.N.Bhanu Prakash[5]

, [1, 2, 3, 4] Assistant Professor, Department of Electrical and Electronics Engineering, Vaagdevi College of Engineering, Warangal, Telangana-506005, India.

5 Professor, Department of Electrical and Electronics Engineering, Vaagdevi College of Engineering, Warangal, Telangana-506005, India

Abstract:
Wide area monitoring (WAM) presents numerous opportunities to enhance power system protection performance. This paper explores these opportunities and their underlying motivations, which include assessing relay characteristics suitability, implementing supervisory control of backup protection, developing more adaptive and intelligent system protection, and creating innovative system integrity protection schemes. While the primary protection requires swift response times, WAM can significantly aid in backup and system protection. The evolving challenges in modern power system protection, such as the increasingly variable operating conditions and the risk of mal-operation of relays, highlight the importance of leveraging WAM for enhanced protection. Supervision of backup protection can mitigate the risk of blackouts, as relay mal-operation contributes to a significant percentage of blackout incidents. Moreover, the growing interconnection and complexity of power systems make them more vulnerable to wide area disturbances, necessitating the implementation of new, adaptive system integrity protection schemes to safeguard power system security.

Keywords: *Backup protection, Blackouts, Hidden failures, Power system protection, System integrity protection schemes, Wide area monitoring, Wide area protection*

1 Introduction:

Wide area monitoring (WAM) stands as a pivotal advancement in modern power systems. Enabled by synchronized measurement technology and Pharos Measurement Units (PMUs), WAM provides a real-time glimpse into the dynamic behavior of power systems, updating once per cycle. This real-time information serves as a vital resource for developing new applications that can enhance power system protection and control. Recent blackout reports have underscored the deficiencies in protection systems, emphasizing the potential role of WAM in bolstering power system protection. However, the high-speed response demanded by primary protection renders wide area measurements unsuitable for this purpose. Furthermore, the necessity for wide area measurements in primary protection is limited, as it primarily safeguards specific elements of the power system. However, aspects of power system protection with lower speed of response requirements (e.g., backup protection) and less selectivity can benefit from wide area measurements to supervise their behavior. Moreover, wide area measurements can serve as the foundation for creating adaptive system protection, innovative system integrity protection schemes, or entirely new protection concepts.

Wide area measurements alone are insufficient to realize these potential enhancements. The advent of digital relays has introduced an unprecedented level of computational power in substations, vastly expanding the functionality of protection systems. This increased capability is shifting intelligence and decision-making from the control center to the substation, paving the way for new protection concepts. However, alongside increased computational power and the availability of wide area measurements, a crucial requirement for any wide area application is a suitable communication infrastructure to support it.

The communication needs of various Wide Area Protection (WAP) concepts can vary significantly. Some may necessitate streaming measurements from multiple locations at a rate of once per cycle (e.g., intelligent controlled islanding), while others may only require binary signals to be streamed at lower rates (e.g., supervision of backup protection). Additionally, the communication infrastructure must meet requirements beyond bandwidth. Low latency and jitter are essential to provide reliable, high-speed responses, and ensuring cybersecurity is vital to prevent WAP from being exploited by malicious third parties seeking to disrupt the power system. Therefore, thorough evaluation of communication needs should be integral to the design of any wide area protection scheme.

The increasing relevance of WAP is driven by the evolving nature of power systems, influenced by three main factors: the wider range of possible operating conditions due to changing generation mixes and demand-side participation; increased interconnection of power systems, with larger inflows from neighboring systems and reduced operating margins due to economic pressures; and the growing complexity and diversity of transmission technology and control (e.g., HVDC, thyristor controlled series compensation, increasing interconnection). These changes make it increasingly challenging to select protection settings that adequately compromise for all credible system conditions and contingencies. Additionally, modern power systems are more susceptible to wide area disturbances, necessitating coordinated responses tailored to the entire system's needs rather than inconsistent local responses based on individual system observations.

Reports indicate that 70% of wide area disturbances involve relay mal-operation during their initiation or evolution. These mal-operations can result from poor relay settings or hidden failures in the protection system. Relay mal-operation's role in wide area disturbances must be addressed as a significant concern, given their contribution to several recent blackouts. Managing these wide area disturbances exceeds the scope of most existing protection systems. These factors have spurred the development of new protection concepts supported by WAM. Given the diverse challenges facing protection, these new concepts encompass a wide range of complexity and ambition. Examples include novel System Integrity Protection Schemes (SIPS) capable of deploying extensive actions to prevent cascading failures, adaptive system protection (e.g., adaptive under-frequency load shedding), supervisory schemes enhancing the security of existing backup protection, and methods that augment our understanding of system protection without altering its behavior (e.g., alarming system operators to the risk of false relay characteristic penetration). Recent efforts have not only focused on developing new concepts but also on practically implementing them, such as utilizing the IEEE 1588 standard for substation synchronization in the Guizhou-Duyun Wide Area Protection (WAP) project in Guizhou province, China.

This paper delineates several proposed concepts and their potential contributions to addressing significant threats to power system protection performance, including:

1. The role of cascade failures and wide area disturbances in power system blackouts
2. Ensuring the security of backup relays in the complex operating conditions of modern power systems
3. Limiting the impact of hidden failures revealed under stressed conditions
4. Adapting system protection actions to the true system state
5. Implementing wide area protection for distribution systems

The paper is structured as follows: Section 2 introduces basic aspects of WAM and PMUs, while Section 3 provides further insights into the proposed protection concepts.

2 Wide Area Monitoring

Wide Area Monitoring (WAM) gathers measurements from remote locations across the power system and integrates them in real-time into a comprehensive snapshot of the system. Synchronized Measurement Technology (SMT) is integral to WAM, enabling accurate time stamping of measurements, primarily using timing signals from GPS. These timestamps facilitate easy measurement combination and phase angle measurements using a common reference.

Phasor Measurement Units (PMUs), developed in the early 1980s, are the most widely used form of synchronized measurement technology. PMUs measure voltage and current phasors once per cycle, and the IEEE C37.118 standard outlines the required measurement performance and communication protocol for PMUs. Notably, this standard allows for inclusion of analog and digital values in measurement streams, facilitating streaming of binary status signals and waveform measurements.

The architecture of a Wide Area Measurement System (WAMS) can be complex, and various design examples are available. The latency, jitter, and reliability of the communication network in a WAMS are critical to ensure it can support protection functions effectively. The communication network must ensure that measurements supplied by the WAMS to the protection functions are received quickly, reliably, and with consistent delays to maintain protection quality.

3 Challenges Faced by Power System Protection

Overview of Power System Protection

The primary role of power system protection is to disconnect faulty or overloaded elements to prevent damage, degrade system security, and protect surrounding areas from danger. Equipment protection is primarily achieved through breaker operations, categorized into primary and backup equipment protection.

Primary protection isolates protected equipment from the system to prevent damage and operates rapidly within 3-4 cycles. Relays used for primary control are often duplicated to prevent failure in fault clearance.

Backup protection clears faults not addressed by primary protection, operating more slowly to ensure proper coordination and offering less selectivity. Setting backup protection is challenging as it covers a larger part of the system and depends more on system operating conditions.

Protection design must balance dependability and security. Dependability ensures the protection system operates when needed, while security ensures it does not operate when unnecessary. Achieving this balance is crucial for protection engineers.

Protection operations are evaluated based on correctness and appropriateness. Correct relay operation aligns with its design, while appropriate action positively contributes to power system security. Evaluating relay operations based on correctness and appropriateness provides insight into their effectiveness.

In addition to equipment protection, safeguarding against partial or total loss of supply/integrity due to phenomena such as transient angle instability, small signal instability, frequency instability, and voltage instability (both short and long term) and cascading outages is essential. This system protection involves actions beyond breaker operations, including measures like under-frequency load shedding (UFLS). Similar to backup protection, system protection operates more slowly than primary protection and its settings are highly dependent on operating conditions.

Traditional protection schemes operate as self-contained entities, utilizing independent local measurement chains. However, with the increasing complexity of power systems, System Integrity Protection Schemes (SIPS) have emerged, utilizing wide area measurements to deliver more sophisticated functionality.

The measurements used by each protection system vary significantly in terms of type, acceptable delay, reporting rate, resolution, and accuracy. SIPS are specifically designed to protect the system from predetermined contingencies, employing a set of predefined actions based on offline system studies. These actions are executed when specific input conditions are met, extending beyond simply isolating the faulted elements.

Conditions triggering SIPS operation can include events (such as line loss), system response (e.g., measured frequency dropping below a threshold), or a combination thereof. Typically, SIPS are armed by one condition and triggered by another. The adoption of SIPS is widespread, with an increasing number of schemes being designed and implemented globally.

Ensuring compatibility and coordination of protection across neighboring systems is crucial, particularly as systems become more complex, expansive, and adaptive. This helps prevent undesirable interactions that could lead to hidden failure modes or direct maloperation.

Cascade failures in power systems occur as a sequence of failures, where each subsequent failure is triggered by the consequences of the preceding ones, such as a series of line trips due to thermal limit violations. While the initiating event of a cascade can often be identified during post-mortem analysis, recognizing it during operation is more challenging. These cascades can unfold rapidly after the initial event and have been implicated in recent blackouts. Preventing such cascades requires fast, adaptive actions beyond the capabilities of most existing power system protection mechanisms.

Local protection, relying solely on local information, cannot assess the entire system's state or needs. Therefore, leveraging wide area information and real-time measurements to develop protection actions designed to safeguard power system security from wide area disturbances is attractive. Such protection must identify stressed conditions that may render the system vulnerable to cascades and potential initial triggering events within the system.

For instance, local protection may promptly relieve a thermal overload to protect an asset, but it may not consider the overload's severity relative to the asset's importance to system security. Immediately removing this asset protection could initiate a cascade of thermal overloads. In contrast, a wide area protection scheme, utilizing wide area measurements to assess the system's state and evolving security threats, could delay local protection actions using dynamic thermal line ratings, thus providing more time to address overloads through alternative means and preserving system security. Wide area protection can thus adapt protection actions to the system's security needs and mitigate wide area disturbances and cascading failures.

Furthermore, the complexity of wide area disturbances and their rapid onset may surpass human operators' ability to manage them effectively. In this context, automatic actions are necessary to maintain system security, with wide area protection offering a means to implement such actions.

Incorrect operation of protection relays has contributed to cascade failures and blackouts. Existing protection relays often use fixed characteristics that do not adjust to true system conditions, leading to correct but inappropriate operation. Changes in power system operating practices, such as shifting emphasis on commercial and environmental factors, have exacerbated this issue. With an increasing variety of generation mixes and load flow patterns, determining suitable protection settings for all likely operating conditions and contingencies has become more challenging, particularly for backup protection relays.

Despite the challenges faced by modern power system protection and the increasing complexity of protection, modern protection performs very well, and almost all relay operations are correct and appropriate. However, incorrect protection actions have played a role in initiating and propagating several major blackouts. A common theme in these events is the presence of hidden failures that cause a relay to operate incorrectly immediately after another protection action has been taken in their local area.

A hidden failure is defined as a permanent, undetected defect in a protection relay that causes a relay to operate incorrectly and remove elements of the system as a consequence of another switching event in the system. Hidden failures are random events that are not indicative of bad relay design. They do not immediately lead to an incorrect operation but will cause one when another event occurs in their local area.

Hidden failures only include those failures that cause a relay to operate incorrectly. Failures that cause the relay to not operate are not hidden failures, as they should be accommodated by redundant protection. Similarly, failures that cannot be monitored are not hidden failures; they are faulty design, and temporary failures that occur during switching are not hidden failures.

Figure 1 presents a comparison of a hidden failure and a non-hidden failure for a three-zone step distance relay. A failure of the contacts of T3 that causes them to be permanently closed will create a hidden failure. This is because the failure of T3 does not cause an immediate maloperation, as Z3 must also be closed. However, in the event of a fault, the line will be immediately tripped without delay when Z3 closes in the presence of any fault in Zones 1-3.

In contrast, a failure of the contacts of Z1 that causes them to be permanently closed will not create a hidden failure. This is because at the instant of the failure, the line will be tripped. While this is a maloperation, it is not a hidden failure, as it immediately caused the line trip.

Possible hidden failures include relay contacts that are always open or closed, timers that operate instantaneously regardless of the set delay, outdated settings, settings that are unsuitable for the prevailing conditions, and human error in relay coordination.

Hidden failures are a particular threat because they require another event in the local area to reveal them. This means that a hidden failure and its triggering event represent two related failures, which is a far more severe threat than two random, unrelated failures. Furthermore, the triggering event itself is usually a sign that the power system is experiencing stressed

conditions. These factors mean that hidden failures inherently threaten to contribute to a cascade of failures in their local area.
Top of Form

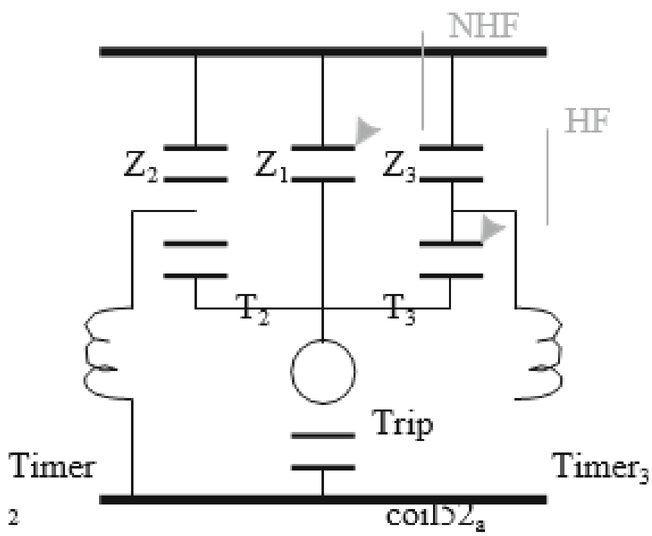

Fig. 1 Example of a hidden failure (HF)andanon-

Hidden failures (HF) for a three-zone step distance relay, as mentioned in [26], are repeated here. The local area was more strictly defined as a region of vulnerability in [25] and will vary significantly for different modes of hidden failure in different elements. The design of any protection scheme directly influences the likelihood of experiencing hidden failures. The urge of wide-area protection schemes may mean that their region of vulnerability could be significantly larger than those seen for existing protection. Therefore, the hidden failure modes and region of vulnerability of a wide-area protection scheme should be rigorously assessed to ensure that their presence does not weaken the protection of the system as a whole.

The greater complexity of System Integrity Protection Schemes (SIPS) and Wide Area Protection (WAP), compared to traditional protection, will mean that analyzing them for hidden failures will be more challenging. A particular challenge involved in analyzing WAP will be the analysis of the wide-area monitoring and communication networks on which they depend. These networks can be highly complex and depend on a wide variety of multi-vendor hardware and technologies. Furthermore, the broader scope of actions available to a SIPS and WAP (e.g., system separation) will mean that the impact of any hidden failure modes may be far greater than it would be for other protection elements.

Considering the increased complexity of analyzing SIPS and WAP to identify hidden failures and the greater consequences of their maloperation, it is particularly important that they are designed with the minimization of hidden failure modes in mind alongside the ability to self-diagnose failures and adapt to them. These considerations should extend beyond the original design to include the development of maintenance procedures.

Hidden failures can only be detected when they cause an incorrect operation or when the faulty element is tested. Ongoing maintenance, calibration, and review of protection could identify existing hidden failures and correct them. Recent work has presented a number of such

methods. However, given the number of protection elements, this ongoing task may be difficult to deliver with the resources available. Therefore, it may be attractive to develop more methods for exploiting the ability of digital relays to self-diagnose the presence of failure modes. Furthermore, Wide Area Monitoring System (WAMS) based concepts for detecting these failures, like those proposed in [29], that can identify such failures may be necessary.
However, it is known that maintenance is a source of hidden failures. Therefore, it is important to develop WAP concepts that can help to limit the impact of hidden failures when they are revealed. Furthermore, recent work, e.g., [30, 31], has incorporated hidden failures into the statistical modeling of power system reliability using expert systems, importance sampling, neural networks, and fuzzy logic. A review of this work is provided in [29].

4 Enhancing Protection with Wide Area Monitoring

The overall objective of using wide area monitoring to enhance protection is to create new protection concepts that will make blackouts less likely to occur and less intense when they do occur. The key areas in which WAM can contribute to power system protection are as follows:

1. Avoiding inappropriate relay settings for the prevailing system conditions.
2. Managing wide area disturbances.
3. Mitigating the impact of hidden failures.
4. Ensuring a suitable balance between the security and dependability of protection.

The primary goal of protection in a power system is to safeguard individual elements from damage while ensuring the overall security of the system. While wide area monitoring has limited applicability in primary equipment protection due to the need for rapid response, it can significantly enhance backup protection, which operates with a slower response time and covers larger zones of the system.
In ensuring the system's resilience against extreme conditions and wide area disturbances, a high level of built-in redundancy and strength is crucial. However, such over-engineering is often not feasible given economic and environmental constraints. Here, wide area monitoring-enhanced protection can play a vital role by enabling system operators to maintain the desired level of security and reliability under these evolving operating conditions.
Wide area measurements provide a platform for developing supervisory schemes for backup protection, advanced forms of system protection, and entirely new protection concepts. Examples include adaptive relays that adjust settings based on system changes, improved protection of multi-terminal lines, and adaptive end-of-line protection strategies.
One such application is alarming against the risk of relay characteristic penetration. This involves detecting when the impedance observed by a relay approaches its characteristic under non-faulty conditions, signaling protection engineers about potentially unsuitable relay settings. While this concept doesn't directly enhance protection performance or utilize wide area measurements, it leverages the communication network required for wide area monitoring to provide valuable information for improving protection security and reliability, especially for critical relays vulnerable to load encroachment or power swings. and otherwise, to ensure that the overall system reliability is not compromised.
To address the issue of load encroachment on impedance relays, which has been implicated in recent blackouts, real-time measurements of the load can be utilized to adjust relay inputs and prevent encroachment. Traditional relay settings are based on offline simulations of anticipated operating conditions and contingencies, making them vulnerable to unforeseen variations in

system conditions, particularly in modern power systems with significant intermittent generation. By leveraging the computational power of digital relays and real-time load measurements, relay settings can be dynamically adjusted to accommodate changing load conditions and mitigate the risk of load encroachment.

Balancing the demands of dependability and security in protection design presents another significant challenge. While existing protection systems prioritize dependability, favoring the reliable clearing of faults under normal operating conditions, they may inadvertently trigger incorrect tripping operations during wide area disturbances, exacerbating stressed conditions and potentially leading to blackouts. To address this, wide area measurements can be used to detect stressed conditions and dynamically adjust the protection philosophy to prioritize security over dependability. By employing logical combinations of relay outputs based on supervisory signals derived from wide area measurements, the protection system can adapt its response to changing system conditions, reducing the likelihood of incorrect tripping operations without compromising overall system reliability.

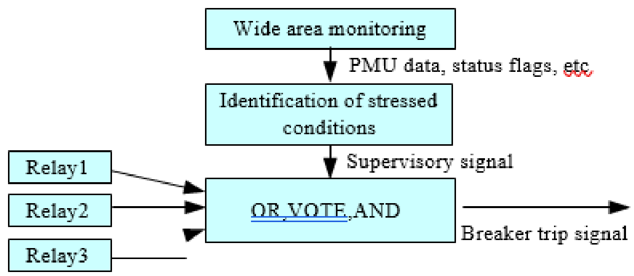

Fig.2The use of WAM to vary the balance between dependability and security

This adaptive protection approach also offers a promising solution to mitigating the impact of hidden failures in protection systems. By requiring multiple relays to concur before initiating a tripping operation, the system can effectively mitigate the risk of a single hidden failure causing incorrect tripping. However, the introduction of such adaptive protection mechanisms must be carefully evaluated to ensure that they do not introduce new failure modes or compromise overall system reliability. The backup relay does not operate, indicating that the fault is outside of its zone of protection. However, if one or more remote PMUs detect the fault, they communicate this information to the backup relay, triggering its operation.

This approach effectively enhances the security and selectivity of backup protection by utilizing wide area measurements to supervise the operation of the relay. By incorporating signals from remote PMUs, the backup relay can make more informed decisions, reducing the likelihood of undesired tripping events caused by maloperation or miscoordination. Additionally, the use of negative sequence currents adds another layer of protection, as they can help distinguish between internal faults and external disturbances, further improving the reliability of the backup protection scheme.

Overall, this method demonstrates how wide area measurements can be leveraged to enhance the performance of backup protection, addressing vulnerabilities such as zone 3 relay maloperation while maintaining system reliability and stability. By integrating remote PMUs and utilizing advanced signal processing techniques, backup protection can be made more robust and responsive to dynamic system conditions, ultimately reducing the risk of cascading failures and blackouts.

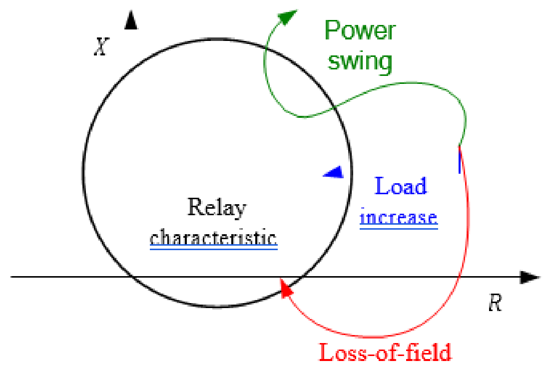

Fig.3Examples of dynamic conditions that can cause maloperation of distance relays[32]

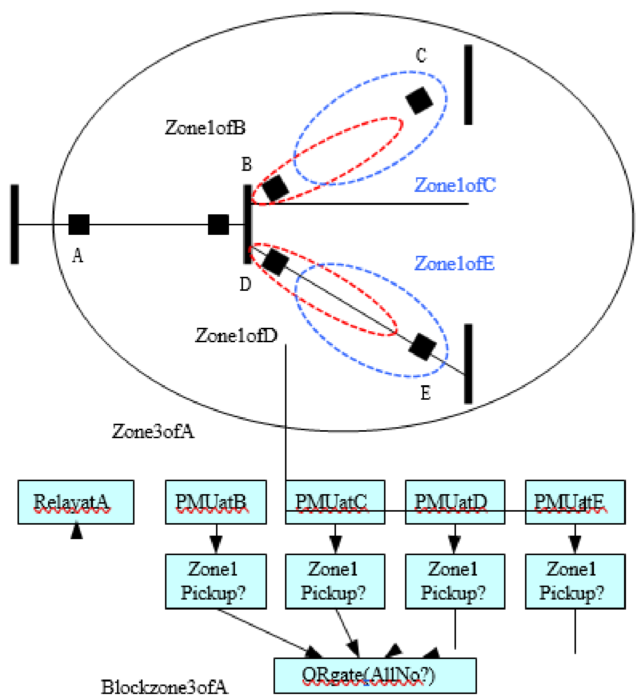

Fig. 4Supervision of backup relay operation using remote PMUs to check for a fault in Zone3 [35]

However, the effectiveness of traditional out-of-step relaying can be limited by the reliance on local measurements and pre-defined thresholds, which may not capture the dynamic behavior of the entire system during extreme events. To address this limitation, adaptive out-of-step relaying schemes have been developed, leveraging wide area measurements to enhance the detection and prevention of out-of-step conditions.

These adaptive schemes continuously monitor system dynamics using synchronized measurements from multiple locations across the power system. By analyzing the phase angles, frequencies, and other relevant parameters from these measurements, the relaying scheme can dynamically adjust its operation to better align with the evolving system conditions. For example, rather than relying solely on predefined impedance zones, the adaptive relays can use real-time information to detect abnormal power swings or changes in system stability, triggering appropriate protective actions.

Furthermore, the use of wide area measurements enables these relays to anticipate and respond to out-of-step conditions more effectively, reducing the risk of system collapse and blackouts. By incorporating advanced signal processing algorithms and machine learning techniques, these relaying schemes can adapt to a wide range of system behaviors and contingencies, enhancing overall system reliability and stability.

Overall, the development of intelligent under frequency load shedding and adaptive out-of-step relaying represents significant advancements in power system protection, leveraging wide area measurements and advanced analytics to improve the resilience and performance of power grids in the face of extreme events and disturbances.

5 Conclusion

Wide area monitoring (WAM) presents a range of opportunities for enhancing the backup protection and system protection of modern power systems. By leveraging synchronized measurements from multiple locations across the grid, WAM enables the development of advanced protection schemes that can address various challenges faced by power system operators.

One significant advantage of WAM-enhanced protection is the reduction in the likelihood of mal-operation of backup relays, which can occur during extreme events and disturbances. Additionally, WAM can help limit the impact of hidden failures, which are often undetected defects in protection relays that can lead to incorrect operations and contribute to system instability.

Moreover, WAM enables the creation of new tools for managing wide area disturbances, allowing operators to detect and respond to system-wide issues more effectively. By providing a comprehensive view of the power system's state and dynamics, WAM-enhanced protection schemes can improve the resilience of power systems against stressed conditions and disturbances, ultimately reducing the frequency and intensity of blackouts.

Overall, the deployment of WAM-based protection concepts should lead to more robust and reliable power systems, with the ability to quickly identify and mitigate potential threats, ensuring the continued delivery of electricity services to customers.

REFERENCES

[1] Phadke AG, Thorp JS, Adamiak MG (1983) A new measurement technique for tracking voltage phasors, local system frequency, and rate of change of frequency. IEEE Trans Power Appar Syst 102(5):1025–1038

[2] Terzija V, Valerde G, Cai DY et al (2011) Wide-area monitoring, protection, and control of future electric power networks. Proc IEEE 99(1):80–93

[3] Chakrabarti S, Kyriakides E, Bi TS et al (2009) Measurements get together. IEEE Power Energy Mag 7(1):41–49

[4] Phadke AG (2002) Synchronized phasor measurements - a historical overview. In: Proceedings of the IEEE PES transmission and distribution conference and exhibition 2002: Asia Pacific, vol 1, Yokohama, Japan, 6–10 Oct 2002, pp 476–479

[5] Phadke AG (2008) The wide world of wide-area measurement. IEEE Power Energy Mag 6(5):52–65
[6] Phadke AG, Thorp JS (2008) Synchronized phasor measurements and their applications. Springer Science & Business Media, Boston
[7] US-Canada Power System Outage Task Force (2004) Blackout 2003: Final report on the August 14, 2003 blackout in the United States and Canada: Causes and recommendations. Office of Electricity Delivery & Energy Reliability, Washington, DC
[8] Report of the Enquiry Committee on grid disturbance in northern region on 30th July 2012 and in northern, eastern & north-eastern region on 31st July 2012. The Enquiry Committee, Ministry of Commerce and Industry, Government of India, New Delhi, India, 2012
[9] Karlsson D, Broski L, Ganesan S (2004) Maximizing power system stability through wide area protection. In: Proceedings of the 57th annual conference for protective relay engineers, College Station, TX, USA, 30 Mar–1 Apr 2004, pp 403–418
[10] Horowitz SH, Phadke AG (2006) Third zone revisited. IEEE Trans Power Deliv 21(1):23–29
[11] Ding L, Gonzalez-Longatt FM, Wall P et al (2013) Two-step spectral clustering controlled islanding algorithm. IEEE Trans Power Syst 28(1):75–84
[12] Phadke AG, Thorp JS (2010) Communication needs for wide area measurement applications. In: Proceedings of the 5th international conference on critical infrastructure (CRIS'10), Beijing, China, 20–22 Sept 2010, 7pp
[13] Begovic M (2004) Wide area protection and emergency control. In: Proceedings of the 2004 IEEE PES power systems conference and exposition, vol 3, New York, NY, USA, 10–13 Oct 2004, pp 1776–1777
[14] Shi BN, Zhang DN, Hu J (2015) Preliminary investigation in wide area protection implementation using IEEE 1588 precision time protocol. In: Proceedings of the IEEE international symposium on precision clock synchronization for measurement, control, and communication (ISPCS'15), Beijing, China, 11–16 Oct 2015, pp 43–47
[15] IEEE Standard C37.118.1 (2011) IEEE standard for synchrophasor measurements for power systems
[16] IEEE Standard C37.118.2 (2001) IEEE standard for synchrophasor measurements for power systems
[17] Terzija V, Regulski P, Kunjumuhammed LP, et al (2011) FlexNet wide area monitoring system. In: Proceedings of the 2011 IEEE power and energy society general meeting, San Diego, CA, USA 24–29 Jul 2011, 7pp
[18] Cai DY, Wall P, Osborne M et al (2016) Roadmap for the deployment of WAMPAC in the future GB power system. IET Gener Transm Distrib 10(7):1553–1562
[19] Horowitz SH, Phadke AG (2006) Blackouts and relaying considerations — relaying philosophies and the future of relay systems. IEEE Power Energy Mag 4(5):60–67
[20] System protection schemes in power networks. Task Force 38.02.19, CIGRE, Paris, France, 2001
[21] Defense plan against extreme contingencies. Task Force C2.02.24, CIGRE, Paris, France, 2007
[22] Thorp JS, Phadke AG (1999) Protecting power systems in the post-restructuring era. IEEE Comput Appl Power 12(1):33–37
[23] Begovic M, Novosel D, Karlsson D et al (2005) Wide-area protection and emergency control. Proc IEEE 93(5):876–891

[24] Cong YH, Wall P, Regulski P et al (2015) On the use of dynamic thermal line ratings for improving operational tripping schemes. IEEE Trans Power Deliv (to be published)
[25] Tamronglak S, Horowitz SH, Phadke AG et al (1996) Anatomy of power system blackouts: Preventive relaying strategies. IEEE Trans Power Deliv 11(2):708–715
[26] Elizondo DC, De La Ree J, Phadke AG, et al (2001) Hidden failures in protection systems and their impact on wide-area disturbances. In: Proceedings of the 2001 IEEE power engineering society winter meeting, vol 2, Columbus, OH, USA, 28 Jan–1 Feb 2001, pp 710–714
[27] Phadke AG, Thorp JS (1996) Expose hidden failures to prevent cascading outages [in power systems]. IEEE Comput Appl Power 9(3):20–23
[28] Zheng TY, Hu ED, Yang H, et al (2016) Fast, in situ demagnetization method for protection current transformers. IEEE Trans Magn (to be published)
[29] Kundu P, Pradhan AK (2015) Online identification of protection element failure using wide area measurements. IET Gener Transm Distrib 9(2):115–123
[30] Lei HT, Singh C (2015) Incorporating protection systems into composite power system reliability assessment. In: Proceedings of the 2015 IEEE Power and Energy Society general meeting, Denver, CO, USA, 26–30 Jul 2015, 5pp
[31] Liu XD, Shahidehpour M, Cao YJ et al (2015) Risk assessment in extreme events considering the reliability of protection systems. IEEE Trans Smart Grid 6(2):1073–1081
[32] Horowitz SH, Phadke AG (2003) Boosting immunity to blackouts. IEEE Power Energy Mag 1(5):47–53