The Consequences of Unauthorised Changes to Protection Relay Settings

Raul Barrera, *Lead Engineer, Voltex Power Engineers Pty Ltd, Australia*

***Abstract*--Basic Protection relays play a critical role in safeguarding electrical power systems by quickly detecting and responding to faults, ensuring the reliability and stability of the grid. However, unauthorised changes to protection relay settings pose a significant threat to the integrity of power systems. This abstract delves into the consequences stemming from such alterations and emphasises the imperative of maintaining the security and integrity of protection relay configurations.**

The paper begins by explaining the pivotal role of protection relays in identifying and isolating faults within a power system. It then scrutinises the potential vulnerabilities that arise when unauthorised changes are made, leading to a cascade of adverse effects on system performance. The consequences encompass compromised fault detection, miscoordination with other protection devices, and increased susceptibility to catastrophic events such as cascading failures and high incident energy arc flash events.

Furthermore, the abstract explores the broader impact of unauthorised changes on the overall reliability of power grids, considering the potential disruption of service, economic ramifications, and compromised safety standards. The paper also addresses the challenges in detecting and rectifying unauthorised alterations, highlighting the need for robust cybersecurity measures and access control mechanisms.

***Index Terms*—protective relaying, cyber security, system reliability, operational downtime, safety hazards.**

I. Introduction

Protection relays are indispensable components of electrical systems, serving as guardians against potential faults and ensuring the reliability and safety of the power grid. These devices are calibrated to respond to specific conditions, providing a crucial layer of defence against overcurrents, short circuits, and other anomalies. However, the consequences of unauthorised changes to protection relay settings can be severe, jeopardizing the integrity of the entire electrical network [1]. This paper explores the ramifications of such unauthorised alterations and underscores the imperative of maintaining the inviolability of protection relay settings.

This work is in support of ICMIAM organised by Dr. Gopinath (Gopi) Chattopadhyay, Postgraduate Programme Coordinator Maintenance and Reliability Engineering and General Chair of ICMIAM2023 at Federation University in Ballarat, Victoria, Australia.

II. The Role of Protection Relays

Please Protection relays play a pivotal role in maintaining the stability and resilience of power systems. These devices are designed to detect abnormal conditions and initiate protective actions to isolate faulty sections, preventing cascading failures and minimising potential damage [2]. Commonly used in substations and critical infrastructure, protection relays are configured with specific settings tailored to the characteristics of the network they are safeguarding.

III. Unintended Consequences of Unauthorised Changes:

A. Compromised System Reliability:

Unauthorised changes to protection relay settings can compromise the reliability of the entire electrical system. Incorrect settings may render the relays ineffective in detecting and responding to faults, exposing the system to the risk of widespread disruptions.

B. Increased Risk of Equipment Damage:

Protection relays are instrumental in preventing damage to equipment by swiftly isolating faulty components. Unauthorized changes may lead to delayed or inappropriate responses, allowing faults to escalate and causing extensive damage to transformers, generators, and other critical assets.

C. Safety Hazards:

Inaccurate relay settings pose a significant safety hazard to both personnel and the public. Failure to promptly isolate faults can result in hazardous conditions, such as electrical fires or electrocution, jeopardizing the well-being of those in proximity to the affected areas. Unauthorised changes to protection relay settings can result in delayed or inappropriate responses to faults. The relays, designed to rapidly isolate faulty sections, may fail to do so effectively, allowing faults to persist and escalate, the duration of an arc flash is a critical factor in determining its incident energy.

An increased incident energy creates safety hazards such as electrical fires, posing a direct threat to both personnel and the surrounding environment [3].

The following example shows a model simulating a protection relay GE Multilin 565 providing device 50, 50G, 51 & 51 G.

FIGURE 1
Overcurrent protection simplified model

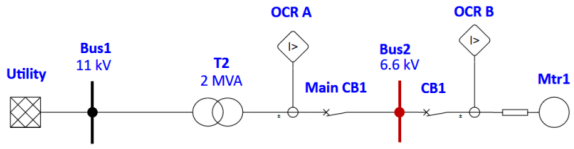

FIGURE 1
Protection settings

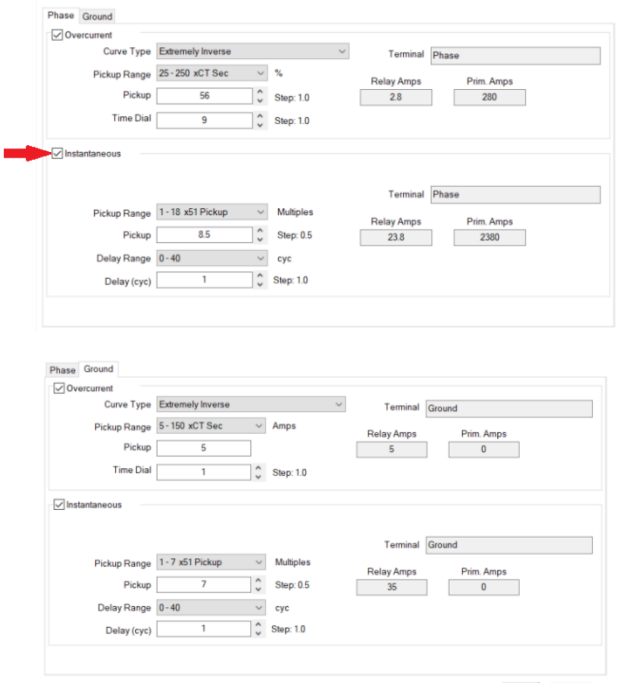

TABLE 1
Arc Flash results

GE Multilin 565		
Instantaneous overcurrent (50)	Enabled	Disabled
Ac Flash Level (Cal/cm2)	A (4)	B (8)
Arc Flash Boundary (m)	0.248	1.19
Incident Energy (Cal/cm2@91.4cm)	0.156	1.8
Fault Clearing Time (s)	0.04	0.472

By disabling the instantaneous overcurrent device (50) the fault clearing time (FCT) increases 11.8 times, calculating the incident energy following IEEE 1584:2018 and using ETAP 22.5 software, the calculated arc flash level increases from A to level B. Recognising that there are various methods and computer tools to estimate arc flash and is inherent risk that may show different outcomes [4], this example demonstrates the issue in question.

D. *Operational Downtime:*

Incorrect relay settings may trigger unnecessary tripping or, conversely, fail to initiate protective actions when needed. Both scenarios can lead to operational downtime, disrupting the normal functioning of industrial processes, commercial activities, and essential services.

IV. ROOT CAUSES OF UNAUTHORIZED CHANGES:

A. *Lack of Security Measures:*

Insufficient access controls and security measures can pave the way for unauthorised personnel to tamper with protection relay settings. Implementing robust monitoring, access controls and authentication mechanisms is crucial in preventing unauthorised access.

B. *Inadequate Training and Awareness:*

Lack of awareness among personnel about the criticality of protection relay settings and the potential consequences of unauthorised changes can contribute to accidental alterations. Comprehensive training programs are essential to ensure that those responsible for maintaining relays understand the gravity of their actions.

V. MITIGATION STRATEGIES:

A. *Access Control and Authentication:*

Implementing stringent access controls, including user authentication and authorisation mechanisms, can help prevent unauthorised access to protection relay settings.

B. *Regular Audits and Monitoring:*

Conducting regular audits of protection relay settings and implementing continuous monitoring systems can detect unauthorized changes promptly. Automated alerts can be set up to notify relevant personnel of any alterations.

C. *Training and Awareness Programs:*

Providing comprehensive training programs to personnel involved in relay maintenance can enhance their understanding of the critical nature of relay settings. Creating a culture of awareness around the potential consequences of unauthorized changes is essential.

D. *Documentation and Change Management:*

Maintaining comprehensive documentation of protection relay settings and implementing robust change management processes can ensure that any alterations are well-documented, authorized, and tracked.

VI. AUTOMATED INTELLIGENT MONITORING

In the rapidly evolving landscape of electrical engineering, the integration of automated intelligent protection relay monitoring systems represents a groundbreaking advancement.

A. *Real-Time Monitoring:*

Automated systems enable real-time monitoring of protection relays, providing continuous surveillance of electrical parameters. This instantaneous feedback allows for prompt detection of anomalies, enhancing the system's responsiveness to potential faults.

B. Data Analytics and Pattern Recognition:

Intelligent monitoring systems utilize advanced data analytics and pattern recognition algorithms. By analyzing historical data and identifying patterns indicative of potential issues, these systems can predict and prevent faults before they escalate, thereby minimizing the risk of disruptions.

C. Remote Monitoring and Diagnostics:

Automated systems facilitate remote monitoring and diagnostics, enabling engineers and operators to assess the status of protection relays from a centralized location. This capability not only reduces the need for physical inspections but also allows for quicker response times in addressing emerging issues.

D. Fault Localisation and Analysis:

Intelligent monitoring systems excel in fault localization, pinpointing the exact location and nature of a fault within the electrical system. This precision enhances the efficiency of maintenance efforts, reducing downtime and improving the overall reliability of the system.

E. Integration with SCADA Systems:

Integration with Supervisory Control and Data Acquisition (SCADA) systems enhances the overall visibility and control of the electrical infrastructure. Automated intelligent monitoring seamlessly interfaces with SCADA, providing a comprehensive overview of the system's health and enabling quick decision-making.

VII. Conclusion:

The consequences of unauthorised changes to protection relay settings extend far beyond mere technical disruptions. They pose a threat to the stability, reliability, and safety of personnel. By recognising the significance of this issue and implementing proactive measures, including robust security protocols, training initiatives, and effective monitoring, we can safeguard our power systems and ensure their continued functionality in the face of evolving challenges. The integrity of protection relay settings is paramount, representing an essential component in the resilience and reliability of modern electrical grids.

VIII. Acknowledgment

The authors gratefully acknowledge the contributions of Mick Weston, Voltex Power Engineers General Manager and Paul Songberg, Voltex Power Engineers Senior Electrical Engineer for their work on the creation of this document.

IX. References

[1] E. Koks, R. Pant, S. Thacker, and J. W. Hall, "Understanding business disruption and economic losses due to electricity failures and flooding," *International Journal of Disaster Risk Science*, vol. 10, pp. 421-438, 2019.

[2] J. L. Blackburn and T. J. Domin, *Protective relaying: principles and applications*. CRC press, 2006.

[3] R. A. Jones *et al.*, "Staged tests increase awareness of arc-flash hazards in electrical equipment," in *Record of Conference Papers. IEEE Industry Applications Society 44th Annual Petroleum and Chemical Industry Conference*, 1997, pp. 313-322: IEEE.

[4] A. Lovrenčič, V. Lovrenčić, T. Jordan, M. Engebrethsen, S. Nikolovski, and K. Cheng, "Arc Flash Risk Assessment according to different Standards Using Several Software Tools," in *2022 13th International Conference on Live Maintenance (ICOLIM)*, 2022, pp. 1-6: IEEE.

X. Biographies

Raul Barrera
BEng (Mech-Elec) MEngPrac (Power Systems) MIEAust CPEng RPEQ NER MIEEE APEC IntPE(Aus)

Lead Engineer and Auditor for the Voltex Group is a practicing chartered professional mechanical and electrical engineer; and holds a Master of Engineering Practice specialising in Power Systems Engineering. His career spans more than 30 years in engineering practice and 12 years as an accredited Hazardous Area, High Voltage and Safety Management System Auditor. Member of Engineers Australia (EA), Senior member of the Institute of Electrical and Electronics Engineers (IEEE) and member of The Electric Energy Society of Australia (EESA)..