Advancement of Safety Features for Industrial Power System Operations and Control

Bhairavi Pandya
Actalent Services

Anil Pandya
Tengizchevroil

Paulo Franco and Chetan Kansagara
Schweitzer Engineering Laboratories, Inc.

This paper was presented at the 71st Annual IEEE IAS Petroleum and Chemical Industry Technical Conference, Orlando, FL, September 11–14, 2024.

For the complete history of this paper, refer to the next page.

Presented at the
71st Annual IEEE IAS Petroleum and Chemical Industry
Technical Conference (PCIC)
Orlando, Florida
September 11–14, 2024

ADVANCEMENT OF SAFETY FEATURES FOR INDUSTRIAL POWER SYSTEM OPERATIONS AND CONTROL

Bhairavi Pandya
IEEE Member
Actalent Services
575 N Dairy Ashford Rd, Ste 600
Houston, TX 77079, USA
bpandya@actalentservices.com

Anil Pandya
Tengizchevroil
QV1 Building
250 St. Georges Terrace
Perth, Western Australia 6000 Australia
anil.pandya@tengizchevroil.com

Paulo Franco
IEEE Member
Schweitzer Engineering Laboratories, Inc.
3050 W Agua Fria Fwy Ste 130
Phoenix, AZ 85027, USA
paulo_franco@selinc.com

Chetan Kansagara
Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Court
Pullman, WA 99163 USA
chetan_kansagara@selinc.com

Abstract—For safe operation of electrical systems at various voltage levels, implementation of various interlocks is arguably as important as protective relaying. This paper chronicles the evolution of the various mechanical and electrical interlocks that build inherent safety in the operation of switchgear. This is accompanied by development of complex logics within the protective relays and their communications over fiber-optic networks that reduce the number of required control cable installations, the potential points of physical failure, and the ongoing maintenance effort. The paper begins with an overview of the industry practice common to most balanced, polyphase power systems. This is followed by specific features that apply to various types of switchgear.

A case study of a state-of-the-art interlock system on a large oil and gas facility, where every electromechanical action of the switchgear interlocks is mimicked by the power management system, is discussed. This includes not only the mechanisms present within the switchgear at each voltage level, but those necessary across various voltage levels.

This paper aims to simplify the understanding of power system interlocks and their interactions with protection and control systems by providing rule-of-thumb guidelines and innovative solutions incorporated in modern power systems, improving operational safety and reliability of the power systems.

Index Terms—Safety Interlocks, Hierarchy of Controls for Hazard Mitigation, Engineering Controls, Relay-Based Interlocks, SCADA-Based Interlocks, Electrical Safety

I. INTRODUCTION

Consider the following statistic: around five percent of all electrical faults are bolted three-phase faults [1]. While in many cases such faults evolve from a single-line-to-ground fault, they are sometimes rooted in human error [2]; for example, the accidental energization of a circuit by closing a circuit breaker while a temporary connection to the ground via a ground switch is still in place. While reliable protective relaying is expected to isolate the fault, implementation of safety interlocks can prevent such undesired operations in the first place.

This paper looks at the evolution of electrical safety mechanisms outside of protective relaying that prevent maloperations when applied correctly. The discussion begins with a layered approach to electrical safety [3]. An overview of the evolution of built-in interlocks is provided, ranging from simple, locally active mechanical arrangements that require little intervention to the utilization of various analog and digital signals in automation-based control schemes that rely on communications protocols. While the importance of well-written operating procedures cannot be overstated as an integral part of electrical safety, they are out of the scope of this paper. A large-scale industrial power system is discussed as a case study.

II. BACKGROUND

Safety is of paramount importance when it comes to the operation and maintenance of any electrical system, given the dire consequences of a safety failure. The concept of electrical safety was first formalized in the United States with the commercialization of electricity. The founding of the National Fire Protection Association, which publishes the National Electrical Code, marks the beginnings of modern safety standards [4]. Workplace safety standards for all industries in the United States were put in place with the establishment of the Occupational Safety and Health Administration. Similar standards have been adopted around the world [5]. The regulatory requirements dictated by these standards provide a basis for methods employed to enhance safety in a lot of industrial power system operations.

Fig. 1 represents the hierarchy of controls as a method of mitigating and ranking safeguards to protect workers from hazards [6]. The pyramid is divided into five levels, each representing a different approach to hazard control. In the context of electrical safety, the levels can be summarized as follows:

1. Elimination refers to completely removing the hazard, which can involve using an alternative energy source that eliminates the risks associated with electricity.
2. Substitution refers to replacing the existing hazardous electrical equipment with a safer option.

3. Engineering controls refer to methods that isolate individuals from the hazard by implementing physical changes that make the system safer.
4. Administrative controls involve establishing various policies, procedures, and protocols to reduce electrical hazards.
5. Personal protective equipment (PPE) acts as a form of safe work practice—under no circumstances should it be considered the sole means to a safe operation.

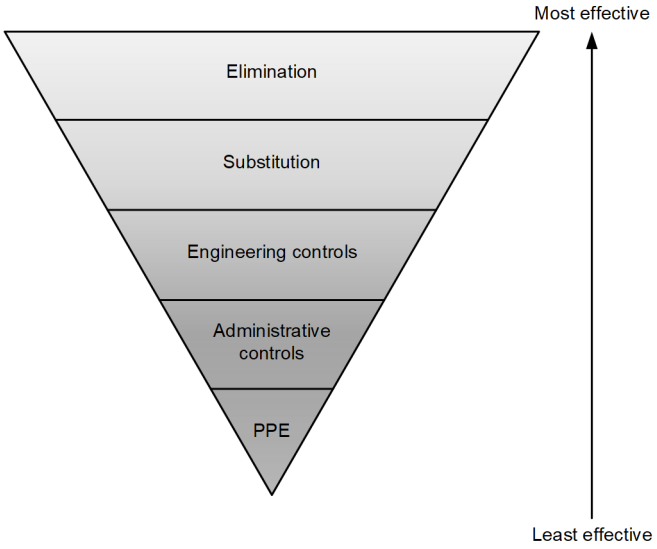


Fig. 1 Mitigating Hazards: Hierarchy of Controls [6]

While equipment and personnel safety are achieved through a combination of the aforementioned methods of hazard control, increased reliance on the first three methods (elimination, substitution, and engineering controls) makes electrical systems inherently safer to operate. Administrative controls and PPE are also critical to the safe operation of any electrical system.

Elimination and substitution as hazard control methods for an energized substation are not directly applicable to industrial power system operation due to the nature of switching procedures to restore or transfer electrical circuits during normal operations. Built-in safety interlocks can be considered as a method of implementing engineering controls, while various operating procedures and signage can be considered administrative controls, with PPE as the last line of defense for those performing the switching operations locally.

While both engineering controls and administrative controls are equally crucial to safe and injury-free operation, this paper focuses on engineering controls, with specific attention to permissive functions at electrical substations and switchgear. Implementing built-in safety mechanisms is a form of engineering control that can prevent unsafe operation and, by extension, reduce the risk to personnel and equipment as well as the associated costs.

Safety interlocks are an effective way to achieve inherent safety in operations. In simple terms, an interlock of any type is a built-in prevention against an undesired outcome.

A. Interlocking Philosophy

Controlled open and close operations for various devices isolate and/or energize different parts of the system. Safety interlocks in a substation or switchgear environment ensure that certain operations, such as closing a circuit breaker or earth switch, can only occur if specific conditions are met. The overall approach to the safe operation of industrial power systems should be considered layered—a combination of devices and actions used to ensure safety. It must be emphasized that these hazard control methods do not intend to replace any administrative or PPE requirements but rather to supplement them. The following is a breakdown of the layers that form the engineering controls:

1. Mechanical interlocks: In their simplest form, these interlocks exist as a mechanical arrangement that allows or blocks operation of a device for certain conditions via mechanical means. A simple example is a ground switch interlocked with a line disconnect switch that uses a bar or a disc to physically block the operation of one when the other is open. There is only one deterministic position for the switch in this case—the line disconnect switch remains open when the ground switch is closed. Conversely, when the line disconnect switch is closed, the earth switch remains open because of the mechanical interconnection.

   While mechanical interlocks are inherently safe and deterministic, their actions are only effective locally and do not take into consideration system conditions, such as the presence or absence of voltage. Their implementation is also highly varied and manufacturer-specific. Their inherently local nature increases reliance on procedures being followed to ensure correct operation at remote ends.
2. Electrical interlocks: These interlocks expand upon the safety features mechanical interlocks provide by accounting for additional system conditions. Such conditions include the absence of any active faults, the presence or absence of a healthy power supply, and device statuses. Electrical interlocks can be roughly categorized in the following three categories; an effective implementation requires that they work together.
   a. Hardwired electrical interlocks: These are wired directly into a control circuit and implemented in a variety of ways. A typical motor start circuit is a simple example of such an arrangement, where the start and stop functions are interlocked with each other by the means of physical wiring, such that only one is functional at a given time.
   b. Relay-based interlocks: These are performed within the primary protective relay. In addition to currents and voltages, microprocessor-based relays receive digital signals indicating the statuses of various devices. These relays can also communicate with other protective relays and exchange signals via peer-to-peer communications methods. The relay then performs logical operations that can be roughly divided into the following categories:

Signals wired to the relay: The analog and digital signals wired to the relays are used to perform logic functions that produce permissive or prohibitive signals, which can be wired into the open or close control circuits of the device in question. Alternatively, the logic functions can be performed within the relay, depending upon the system design.

Signals received via peer-to-peer communications: In addition to the information available locally at the relay terminals, critical information from remote ends of the system can be obtained via communications channels, such as line differential channels or other peer-to-peer communications protocols. For example, information about the status of a circuit breaker or a line disconnect switch located at the other end of the line can be obtained over the communications channels between the two relays and used when operating a ground switch locally. One of the biggest advantages of communications-based interlocks is that their reach extends beyond the substation. This is particularly useful with networks interconnected over longer distances, as the signal exchange often relies on the existing communications networks and does not require dedicated wiring over long distances.

c. Supervisory control and data acquisition (SCADA)-based interlocks: Modern automation systems provide the capability to control and monitor field equipment remotely from the SCADA system over any communications interface available. In addition, they are capable of mimicking the existing relay and communications-based interlocks, preventing the remote operator from issuing a control incorrectly.

B. Influencing Factors

In addition to the built-in functions provided by the manufacturer, system topology, system voltage level, and end-user requirements influence the types of interlocks present in a system. Due to their interconnected nature, impacts of operation at one end further affect other parts of the system.

1. System voltage: Implementation of safety interlocks becomes more complex the higher the voltage level is, due to the increased number of isolation points introduced by the various circuit breakers, disconnect switches, and earth switches within the network topology. This is also because the consequences of an incorrect operation impact a larger part of the electrical system as the system voltage increases.
2. Topology: The complexity of safety interlocks at higher voltage levels is partly due to the interconnected nature of high-voltage (HV) networks where impacts of operation at one area further affect other parts of the system. While still critical for medium-voltage (MV) and low-voltage (LV) levels, these interlocks are often simpler than HV interlocks due to being radial in nature. A lot of close and open operations for circuit breakers at medium and low voltages can be simplified to two factors: the presence of a healthy power supply and the status of the earth switches.
3. End-user requirements: Specific standards for safety interlocks vary based on the end user in an industrial system. The utility feeds coming in at higher voltages delineate the jurisdiction of the utility—at medium and low voltages, there is a lot of variation in how systems are built and operated.

III. CASE STUDY

The industrial system being studied here is one of the world's largest oil and gas field expansions. The newly expanded part of the system operates on a 110 kV transmission network comprising two feeds from the local utility and facility generation. The transmission network then feeds into 10 kV MV switchgears before expanding into lower voltage levels of 380 V. This section discusses the electrical, communications, and SCADA-based interlocks applied to various parts of this system.

A. Switchgear Safety Interlocks

Newly installed HV and MV switchgears throughout the system employ various safety interlocks. Following is an example of HV gas-insulated switchgears (GIS) in breaker-and-a-half bus arrangement. Each circuit with a breaker is referred to as a bay, and each three-breaker arrangement within the bus is referred to as a diameter.

Fig. 2 is a simplified representation of one such arrangement. The breakers connected directly to Bus 1 or Bus 2 are referred to as main breakers, and the breaker contributing to both circuits is referred to as the middle breaker. The main and middle breakers work in conjunction to energize or de-energize various lines fed from the GIS. As discussed previously, the interlocks are implemented in a layered fashion and work in tandem with the detailed operating procedures.

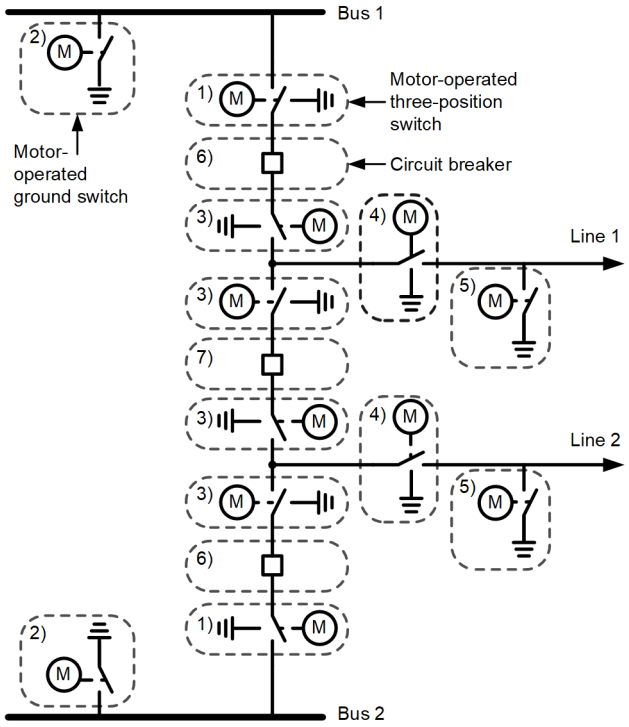


Fig. 2 HV Arrangement

The motor-operated switches, 1 to 5, shown in Fig. 2 are typically three-way switches with the following statuses: closed, open, and grounded. The permissive conditions for open and close operations for the line and ground disconnect switches differ based on the device they connect to. The disconnect switches, 1 to 5, in Fig. 2, are not designed to operate with load and do not have any current-interrupting capabilities like the circuit breakers, which were designed for such operations.

The following section describes the permissive conditions for disconnecting devices shown in Fig. 2.

1. Local/remote switch status: All the disconnecting devices can be operated locally or remotely. When the switch is in local mode, operations from local control panels are allowed, but remote commands originated by SCADA are prevented. Similarly, when the switch is in remote mode, local operations are prevented.
2. Grounded position of the three-position switches (Switches 1, 3, and 4 in Fig. 2) are treated as separate electrical switches. The grounding switch can be operated locally or remotely. Open and close commands take into account the open position of the adjacent breaker disconnect switch (3) and the local/remote switch status.

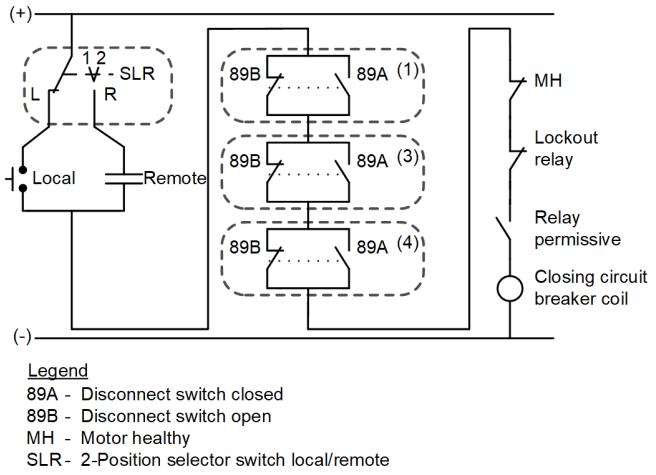
The following conditions are specific to the position and type of each disconnecting device and apply to open and close commands received locally or remotely.

1. Bus disconnect switches (Switch 1): Switches connect the diameters to Buses 1 and 2 via main breakers (Breaker 6). They are allowed to operate under the following conditions:
    a. Operating motor is healthy and powered on.
    b. Main breaker is open (Breaker 6).
    c. Bus ground switch is open (Switch 2).
2. Main breaker disconnect switch not grounded (Switch 3) and bus ground switches (Switch 2): These, like the line ground switches, play an important role in the safe operation of a power system. The bus ground switches are allowed to operate under the following conditions:
    a. Operating motor is healthy and powered on.
    b. All bus disconnect switches related to the bus are open (Switch 1).
3. Circuit breaker disconnect switches (Switch 3): These provide breaker isolation from the line. They are allowed to operate under the following conditions:
    a. Operating motor is healthy and powered on.
    b. Main breakers are open (Breaker 6).
    c. Bus disconnect switch is not grounded (Switch 1).
    d. Line disconnect switch is not grounded (Switch 4).
4. Line disconnect switches (Switch 4): The operation of the line disconnect switches is deemed a critical step as they directly energize the line when closed with availability of supply.
    a. Main breaker is open (Breaker 6).
    b. Middle breaker is open (Breaker 7).
    c. Line ground switch is in open position (Switch 5).
    d. Relay-based permissive conditions are met (discussion to follow).
5. Line ground switches (Switch 5): These play an important role in operational safety as they are specifically designed to ground particular parts of the system. An out-of-sequence or incorrect operation can result in severe consequences, such as undesired trips. These are only allowed to operate when:
    a. Operating motor is healthy and powered on.
    b. Line disconnect switch is in open position (Switch 4).
    c. Relay-based permissive conditions are met (discussion to follow).
6. Main circuit breakers (Breaker 6): These are typically the last pieces of equipment to close and the first to open. It should be noted that operation of the breakers is allowed as long as a deterministic status (fully open or fully closed) of the disconnect switches can be confirmed. Conditions that allow close operation of the breakers are:
    a. Operating motor is healthy and powered on.
    b. Bus disconnect switch is not grounded (Switch 1).
    c. Main breaker disconnect switch is not grounded (Switch 3).
    d. Line disconnect switch is not grounded (Switch 4).

e. Relay-based permissive conditions are met (discussion to follow).

7. Middle circuit breaker (Breaker 7): Similar to the main breaker, it is designed to operate on-load. Conditions that allow close operation of this breaker are:
    a. Operating motor is healthy and powered on.
    b. Surrounding breaker disconnect switches are in fully open or fully closed position.
    c. Line disconnect switch is open or closed (Switch 4) and relay-based permissive conditions are met (discussion to follow).

Among the devices discussed previously, line disconnect switches, ground switches, and circuit breakers are deemed critical to the safety of operation. As a result, additional measures on top of those the manufacturer built in are often employed. These typically come in the form of digital outputs from the relay wired in series with the operating coils of these devices. Fig. 3 shows an example of the main breaker close interlocking schematic diagram. Protective relaying-related checks, such as voltage sense, along with other breaker-specific statuses, such as trip circuit monitors, are omitted from the diagram for simplicity.



Legend
89A - Disconnect switch closed
89B - Disconnect switch open
MH - Motor healthy
SLR - 2-Position selector switch local/remote

Fig. 3 Main Breaker Close Interlocking Example

B. Relay-Based Interlocking

Typically, HV protective relaying is dual-redundant; however, controlled remote open and close commands for the breakers and disconnect switches are deemed less critical than trip commands and are only performed in the primary protective relays. In case the primary relay is out of service, the operator can open the breaker from the local control panel, which does not depend on relays to open the breaker; however, based on the electrical switching procedure, it is not allowed to close the breaker with the primary relay out of service.

In addition to the analog and digital signals directly wired to the relays, modern microprocessor-based relays offer the advantage of communications-based signals exchanged with devices in different parts of the system that may impact the safety of operations.

1. Line disconnect switch permissive (4): As part of the relay-based interlocking, the relay receives and evaluates the status of the remote-end devices.

    As a general rule, the line disconnect switch should be allowed to operate as long as the remote ends are not grounded.

2. Ground switch close permissive: Like the line disconnect switches, ground switch permissive differs with the remote-end configurations.

    As a general rule, operation of a ground switch is allowed when remote-end breakers (and/or line disconnect switches) are open and de-energized.

3. Circuit breaker permissive: With the built-in interlocks, breakers can operate if the positions of the surrounding disconnect switches are deterministic. To ensure safe operation, the following additional checks are performed before issuing a close command:
    a. No trips present
    b. Healthy voltage conditions
    c. Absence of block-close signal

    Voltage checks are performed only in the primary protective relay, which has a three-phase voltage input and two reference voltages. For the main breaker, the reference voltage for synchronism checks comes from the bus potential transformer (PT). When the line disconnect switch is open, the relay allows the breakers to close via both local and remote controls for the following set of combinations for the main breaker:
    a. Dead line—dead bus
    b. Dead line—live bus
    c. Live line—dead bus
    d. Live line—live bus with synchronism check okay

    For the middle breaker, the reference voltage for a synchronism check comes from the line PT on the adjacent bay. Voltage checks for the middle breaker take into account the opposite bay line voltage as the reference voltage. The voltage checks for the middle breaker may be performed in primary protective relays on both ends or just one end, depending upon the system specifications and accounting for the following conditions:
    a. Dead line—dead-opposite line
    b. Dead line—live-opposite line
    c. Live line—dead-opposite line
    d. Live line—live-opposite line with synchronism check okay

    Other conditions to account for are impacted by the configuration of the adjacent devices. For instance, for the breaker-and-a-half scheme, energizing a diameter, and thereby the two lines connected to it, requires special considerations for all three breakers. Similarly, for a specific bay, simultaneous close operation of the main and the middle breakers must be prevented. Closing two breakers at the same time may result in an out-of-sync operation in some cases,

causing mechanical damage and extended system outages. For operational safety, a short time delay must be introduced, in the event that the mechanisms cannot be separated.

4. Peer-to-peer communications permissive: The permissive conditions implemented via the use of communications to other protective relays depend almost exclusively on the remote-end system configuration. For example, the local relay can sense the absence of voltage but cannot distinguish if the remote end is grounded without peer-to-peer communications between both ends. In this case, an HV line can have the following remote-end arrangements:
    a. Short transmission lines: the remote end in this case is at the same voltage level. The configuration for this arrangement can either be an identical breaker-and-a-half scheme on both ends or a different arrangement in the case of older existing networks.
    b. MV feeders: the remote end, in this case, feeds into a step-down transformer that, in turn, supplies MV and LV loads.

To maintain efficiency, the signal exchange over communications is kept minimal. The relays on both ends perform logic functions internally on a combination of local statuses before sending out a permission to operate a disconnecting device. The signals received via communications channels are then utilized in combination with local statuses to operate digital outputs.

Fig. 4 demonstrates a simple representation of various analog, digital, and communications-based signals. The interlocking signal exchange shown here is between two ends of a short transmission line that are both breaker-and-a-half arrangements.

Fig. 5 demonstrates a simple representation of an interlocking signal exchange between an HV breaker-and-a-half arrangement that feeds into an MV load. Similar to the HV-HV interlocks, relays on both ends take into account the local device statuses as well as permissive signals received via communications channels from the other end of the line.

Fig. 4 and Fig. 5 do not show all connections from the primary equipment, such as current transformers, to the protective relays to simplify the schematic.

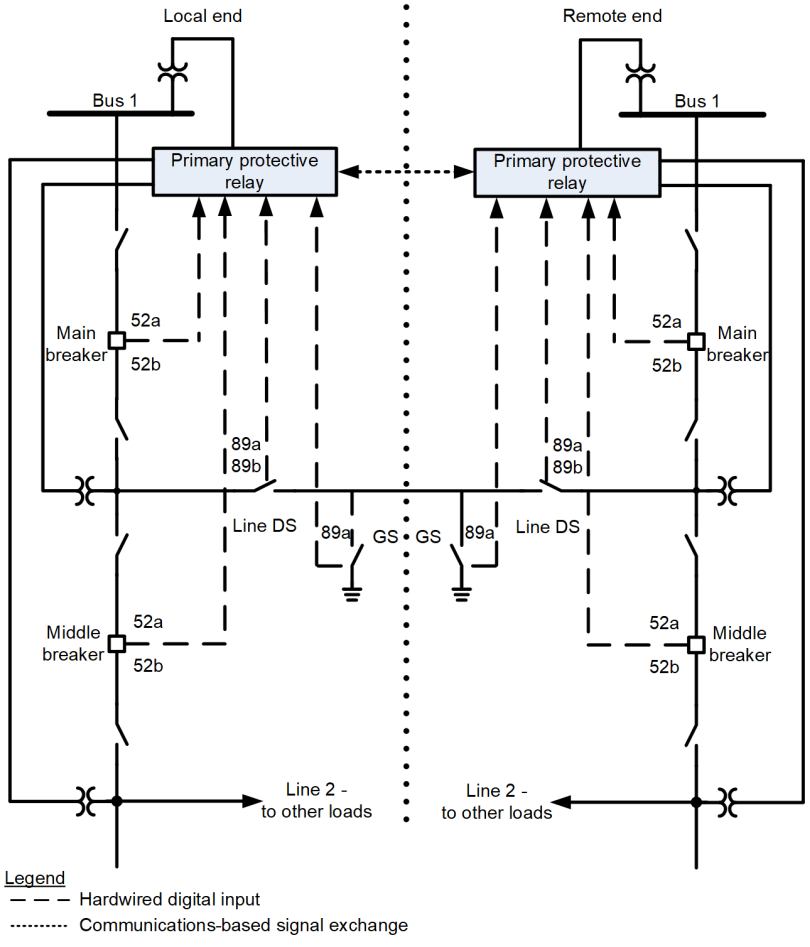


Fig. 4 HV-HV Interlocks Example

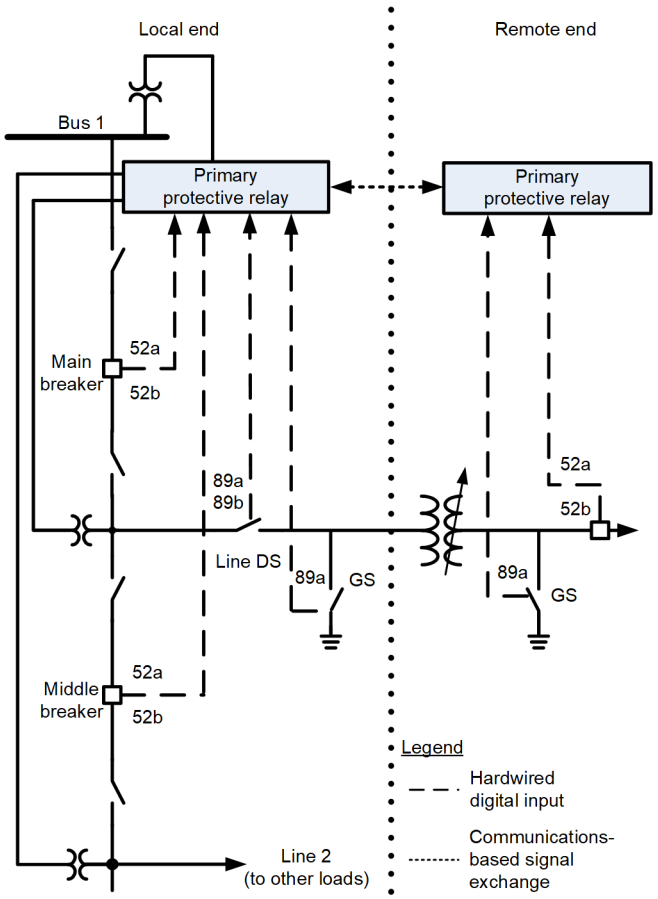


Fig. 5 HV-MV Interlocks Example

Fig. 6 demonstrates a simple representation of interlocking signal exchange between an MV feeder and the LV load connected to it. Relays on both ends take into account the local trip statuses as well as an LV breaker close permissive signal received via communications channels from the other end of the line.

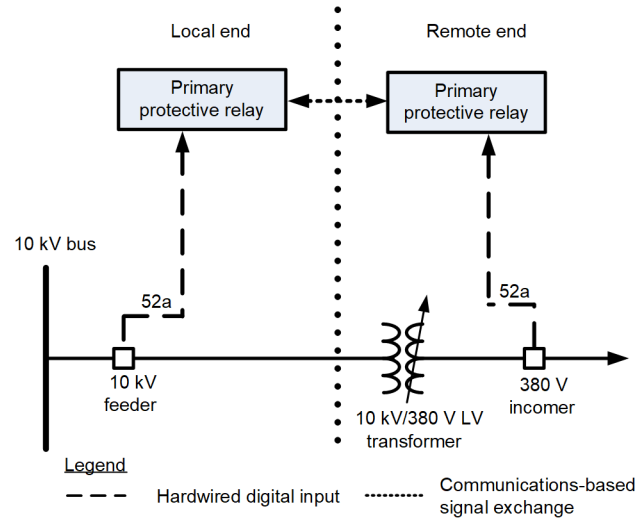


Fig. 6 MV-LV Interlocks Example

Table I, Table II, Table III, and Table IV demonstrate the signals exchanged for configurations demonstrated in Fig. 4, Fig. 5, and Fig. 6. Arguably the most important, but not discussed here, are the intertrip signals exchanged over peer-to-peer communications between relays to and from each end. These are a part of protection schemes and replicated in both primary and backup relays.

TABLE I
HV-HV SIGNAL EXCHANGE OVER COMMUNICATIONS CHANNELS

Signal	Permissive condition
110 kV circuit breaker close permissive	Line disconnect switch closed and ground switch open on remote end
110 kV line disconnector control permissive	Ground switch open on remote end
110 kV line ground switch control permissive	Line disconnect switch open and ground switch closed on remote end

TABLE II
HV-MV SIGNAL EXCHANGE OVER COMMUNICATIONS CHANNELS

Signal	Permissive condition
10 kV ground switch control permissive	Allow closing 10 kV ground switch—110 kV line disconnect switch and 110 kV ground switch open
10 kV circuit breaker close permissive	Allow closing 10 kV incomer breaker—110 kV main or middle breaker closed and 110 kV line disconnect switch closed

TABLE III
MV-HV SIGNAL EXCHANGE OVER COMMUNICATIONS CHANNELS

Signal	Permissive condition
110 kV circuit breaker close permissive	Breaker open condition or breaker closed and line voltage healthy and 10 kV ground switch open
110 kV line disconnector control permissive	10 kV ground switch open
110 kV line ground switch control permissive	10 kV ground switch closed

TABLE IV
MV-LV SIGNAL EXCHANGE OVER COMMUNICATIONS CHANNELS

Signal	Permissive condition
10 kV breaker open	Breaker open

C. SCADA-Based Interlocking

Innovation in electrical interlock techniques comes from power management systems that digitally replicate the types of interlocks described previously to provide an additional layer of safety.

1) Communications Architecture

The communications architecture designed in this case study is a combination topology between dual-ring (solid outline) and star (dashed outline) fiber-optic topologies, shown in Fig. 7, and is not intended to represent all industry standard communications architecture. The LV motor control centers connect via redundant fiber optics to their respective area substations in the star topology. The area substations have HV switchgear or an MV switchboard and, in some cases, both voltage levels are present. The area substation connects directly to a maintenance and operation (M&O) building in the redundant star topology. The redundant M&O building is connected via fiber-optic ring topology, and it supports the necessary infrastructure for the operation, such as firewalls, active directory for user authentication, engineering access for maintenance, and a centralized SCADA for electrical power system operations. The Utility Interface (UI) substation is the only substation directly connected to the ring.

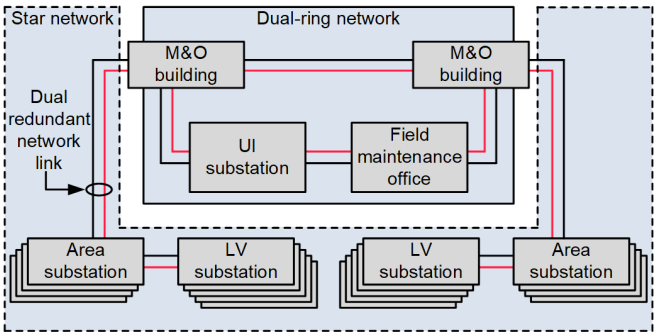


Fig. 7 Overall Communications Architecture

In addition to the centralized SCADA located at the M&O buildings, each area substation has a local human-machine interface (HMI) for operation. The local HMIs are part of the SCADA design, discussed in the following subsections.

2) Data Flow

Modern SCADA and HMI systems support most power system protocols and, in this application, intelligent electronic devices (IEDs) serve data to the HMI, primarily using Distributed Network Protocol (DNP3) and IEC 61850 Manufacturing Message Specification (MMS) protocols. DNP3 is a client/server protocol where the IED is the server and the HMI is the client. DNP3 supports report by exception, whereby changes are transmitted soon after they occur, and an occasional integrity poll is issued to synchronize the client and server databases [7], using network bandwidth efficiently. The MMS is part of the IEC 61850 suite of protocols and works based on client/server architecture. The MMS communications work based on report information between server and client. The pre-identified points inside a data set create reports when data change, quality changes, or data update, as well as periodically [8].

IEDs serve data directly to the primary local HMI (Computer 1) and a remote redundant HMI (Computer 2) all the time. The setup in Fig. 8 ensures data are always available to Computer 1 and Computer 2 at the same time without any delay.

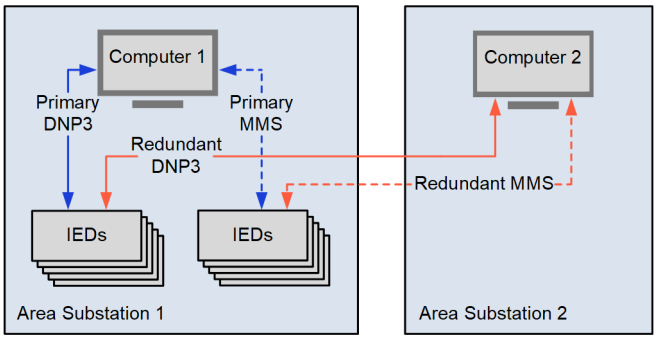


Fig. 8 IED Data Flow

3) SCADA Circular Redundancy

Traditional SCADA redundancy normally requires two computers per station; one computer works as the primary and the other as the standby. Three stations would thus require six computers to provide SCADA redundancy.

Circular redundancy is a logical organization for efficiently connecting several SCADA projects to one another. With circular redundancy, several projects can run simultaneously on one computer. Each computer is the server for one project and, at the same time, the standby server for the neighboring project; additionally, it can be the client for other projects. This results in a circle [9].

As an example, Fig. 9 shows three area substations in a circular redundancy connection. The IEDs located in Area Substation 1 serve data to Computer 1 (primary HMI) and Computer 2 (backup HMI), the IEDs from Area Substation 2 serve data to Computer 2 (primary HMI) and Computer 3 (backup HMI), and the IEDs from Area Substation 3 serve data to Computer 3 (primary HMI) and Computer 1 (backup HMI). Each computer runs two HMI projects with an active interface with the IEDs and a third project as an HMI viewer of the area substation without a direct connection. A logical link between computers manages the circular redundancy; this logical link is responsible for informing the backup HMI projects to archive the data from adjacent IEDs and automatically restore the archived data in the event of the failure of the computer running the primary HMI. It ensures that there are no data losses in the event of a computer failure or scheduled maintenance.

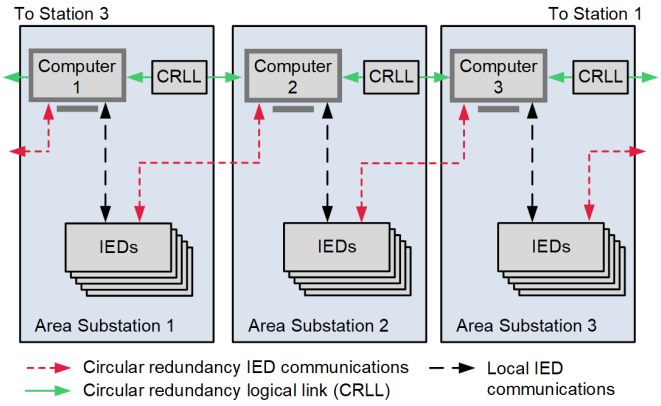


Fig. 9 Circular Redundancy Concept

In addition, the circular redundancy logical link is capable of sharing the data from its primary HMI project with all other computers. This means that from any location, the operator is able to view or control equipment at different locations. Specifically, to prevent inappropriate operations, control from other area substations is not allowed in this design as part of the electrical switching procedure. User commands from adjacent area substations are turned off in the circular redundancy configuration.

4) SCADA Interlocking

One of the features available from the SCADA software package is to allow the user to create custom interlocks depending on the status of selected variables. In SCADA circular redundancy, local station variables are available and systemwide variables can be selected to be part of the interlocking scheme.

Without using any other communications protocol or network resource, it is possible to design a SCADA-based interlocking. As part of the SCADA-based interlocking, the interlocking logic considers the field equipment contact disagreement; for example, the circuit breaker must be open to satisfy the interlocking permissive. Also, for safe operation, the interlocking logic checks the IED communications status to confirm the health variable status and that the position of the local/remote selector switch is in the remote position. Fig. 10 shows an example of the line disconnect switch interlocking implemented as part of the SCADA design, mimicking the hardwire interlocking. For this example, there is no peer-to-peer communications between relays and the status of the ground switch from the remote location is unavailable locally, making it necessary to include the SCADA interlocking logic as part of the switching requirements. The electrical switching procedure must be followed before issuing a command from the local control panel, checking the status of the ground switch from the remote end. As shown in Fig. 10, the SCADA interlocking considers the line ground switch status and its communications status from a different area. The electrical switching procedure must be followed before issuing a command from the local control panel operation.

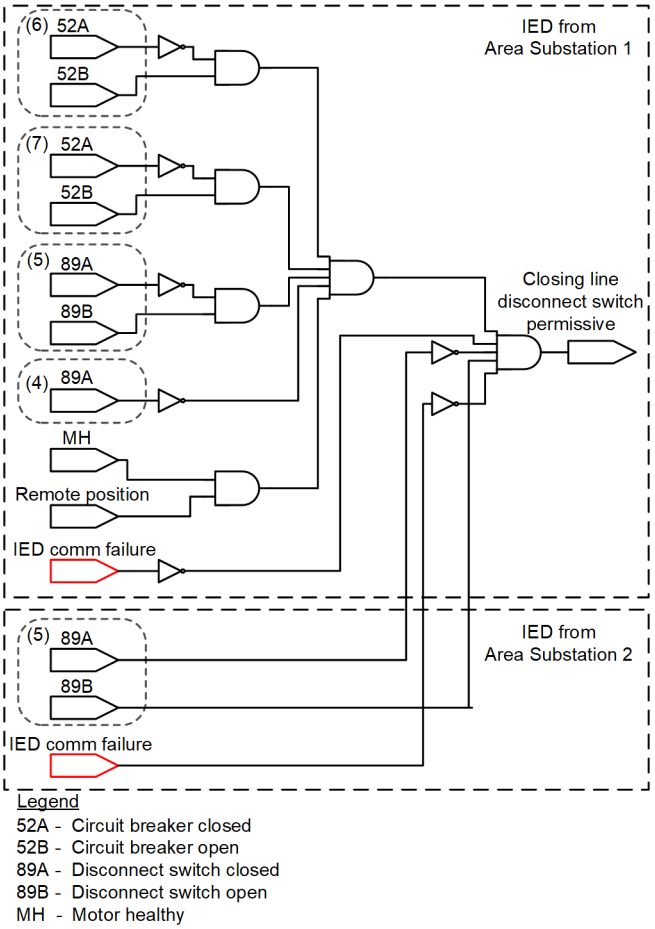


Fig. 10 Typical SCADA Interlocking Based on Circular Redundancy

Fig. 11 shows a typical SCADA-control interface, where the operator has a visual indication when the control buttons are disabled (gray) and clear indication when the controls are available, such as closing the breaker and the breaker disconnect and opening the bus disconnect when the interlocking conditions are satisfied.

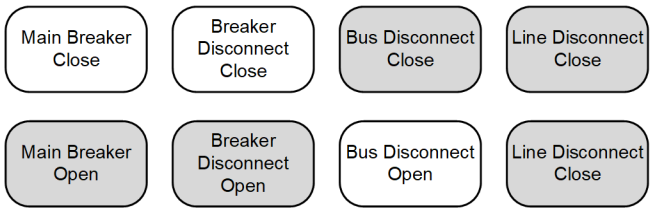


Fig. 11 Typical SCADA-Control Interface

IV. CONCLUSION

The layered approach for implementing electrical interlocks to improve electrical power system operation is highly effective and widely adopted throughout various industrial environments. Administrative controls, such as the electrical switching procedure, depend on human discipline and attention to complying with and following procedures. This paper focuses

on engineering controls as a method to improve the safety of electrical power system operations.

Hardwired electrical and relay-based interlocks go hand-in-hand, checking the electrical system topology and status to allow safe operation locally and remotely, adding the first layer of defense when operating remotely.

SCADA-based interlocks are an important innovation in operational safety in industrial electrical systems. SCADA-based interlocks not only provide greater visibility into the system but also enable the remote operation of various power system equipment, thus enhancing existing engineering controls. This ability to remotely monitor and operate equipment is particularly significant in safety operations, allowing the operator to control the system from a safe location.

V. REFERENCES

[1] J. J. Grainger and W. D. Stevenson, *Power System Analysis*, McGraw Hill, New York, 1994.

[2] M. Ivanova, R. Dimitrova, and A. Filipov, "Analysis of Power Outages and Human Errors in the Operation of Equipment in Power Grids," 12th Electrical Engineering Faculty Conference (BulEF), Varna, Bulgaria, 2020, pp. 1–5, doi: 10.1109/BulEF51036.2020.9326058.

[3] J. Reason, "The Contribution of Latent Human Failures to the Breakdown of Complex Systems," *Phil. Trans. Roy. Soc.* B , Vol. 327, No. 1241, April 1990, pp. 475–484, doi:10.1098/rstb.1990.0090.

[4] *NFPA 70 National Electric Code*, National Fire Protection Association, 2023.

[5] ISO Standard 45001, *Occupational Health and Safety Management Systems: Requirements With Guidance for Use*. Available: iso.org/iso.

[6] J. Z. N. Ajslev, J. L. Møller, M. F. Andersen, P. Pirzadeh, and H. Lingard, "The Hierarchy of Controls as an Approach to Visualize the Impact of Occupational Safety and Health Coordination," *Int. J. Environ. Res. Public Health*, Vol. 19, Issue 5, 2022.

[7] IEEE Std 1815, *IEEE Standard for Electric Power Systems Communications - Distributed Network Protocol (DNP3)*, 2012.

[8] IEC 61850-8-1, *Communication Networks and Systems for Power Utility Automation* – Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3, 2020.

[9] Zenon manual, Service Engine & Engineering Studio - Network - Redundancy, 2022.

VI. VITAE

Bhairavi Pandya is a PE-licensed electrical engineer with over 11 years of experience with a protection focus. Bhairavi has an MSEE from Michigan Technological University with specialization in power systems. She has extensive experience with both domestic and international protection system design and implementation. She leads a team of engineers in her current role at Actalent Services with a main focus on distribution systems and grid modernization. As a protection engineer for Schweitzer Engineering Laboratories, Inc. (SEL), she specialized in industrial protection systems at various voltage levels. She enjoys commissioning protection systems in various environments across the globe and has commissioned projects in the United States, Italy, Indonesia, and Kazakhstan. She has been a member of IEEE since her time as a graduate student. Bhairavi can be reached at BPandya@actalentservices.com.

Anil Pandya is a professional electrical engineer with over 33 years of experience covering various aspects including design, operation and maintenance, engineering and construction of greenfield and brownfield projects from concept to commissioning; HV, MV, and LV power system operation and maintenance; power system protection studies; and relay coordination of electrical networks including power generation. He has worked in the oil and gas industries in Australia and Kazakhstan, power generation and water treatment plants in the United Kingdom, and the fertilizer and petrochemical industry in India and Malaysia. Anil has led the design and execution of grassroots projects and plant upgrades and is skilled in analyzing failures, reviewing protection systems, and implementing remedial solutions to achieve power system reliability. Due to his work with industries where highly flammable gases and liquids are used for various process applications, Anil has gained knowledge of selection, installation, and commissioning of electrical equipment in hazardous areas. Anil can be reached at Anil.Pandya@tengizchevroil.com.

Paulo Franco received his BSEE from Universidade Estadual Paulista Campus de Bauru, Brazil, in 2005. He has experience in electric power protection, integration, automation, communications, control, SCADA, and energy management systems (EMSs). He worked as an automation and commissioning engineer for PEG, where his responsibilities included commissioning, specification, and studies of automation of utilities and industrial plants. In 2007, he joined Schweitzer Engineering Laboratories, Inc. (SEL), where he is currently an automation application engineer.

Chetan Kansagara received his MSEE from the University of Houston. In 2019, he joined Schweitzer Engineering Laboratories, Inc. (SEL), as a project engineer in commissioning where he designs and commissions electrical power plant automation and protection systems. He has extensive experience in troubleshooting and commissioning of power systems' automation and protection systems. He has commissioned projects in United States, Saudi Arabia, South Korea, and Kazakhstan. He brings over eight years of experience as an instrumentation and control system engineer, designing control and safety instrumented systems for onshore and offshore oil and gas facilities.

Previously presented at the 71st Annual Petroleum and Chemical Industry Technical Conference, Orlando, Florida, September 2024.

20240403 • TP7149