Exploring IEEE Std. C37.120-2021 Guide for Protection System Redundancy for Power System Reliability

This paper is a product of the IEEE PSRCC working group C48. The working group consisted of the following members: Alla Deronja (Chair), Melvin Moncey Joseph (Vice-Chair), Kevin Donahoe, Addis Kifle, Craig Palmer, Manish Patel, Juan Piñeros, Solveig Ward, Don Ware

***Abstract*— This paper covers principles of protection system redundancy and summarizes the IEEE C37.120-2021, Guide for Protection System Redundancy for Power System Reliability. This guide has been developed to assist users in applying protection system redundancy; to provide information about which factors to consider when designing redundant protection systems; and to address different approaches to applying redundancy depending on application areas and present practices. General considerations for redundancy are presented including its fundamentals, impact on power system reliability, and the factors affecting redundancy application and design. The effects of various protection system components on redundancy are discussed including instrument transformers, dc system elements, and relay and communication systems. Redundancy application considerations for power system equipment such as generators, buses, transmission lines, and power transformers are provided.**

***Index Terms*— backup protection, breaker failure protection, dependability, IEEE C37.120™, primary protection, protection systems, redundancy, reliability, security**

I. Background

IEEE Power System Relaying and Control (PSRC) Committee working group C31 has developed the *Guide for Protection System Redundancy for Power System Reliability*. This summary paper introduces the new guide to the industry, now referred to as IEEE C37.120-2021.

In 2010, PSRC working group I19 developed a technical report *Redundancy Considerations for Protective Relaying Systems* [2] that initially addressed the issue of protection system redundancy. However, NERC requested PSRC to develop an IEEE guide to streamline and maintain industry compliance with regulatory reliability standards.

II. Introduction

Power system reliability is necessary to maintain the integrity of power systems, and protection systems have a direct effect on reliability. Redundancy addresses failures in the protection system and, therefore, its application helps improve power system reliability.

Each protection system possesses two characteristics that define how it affects power system reliability: dependability (its ability to always operate when needed) and security (its ability to never operate when not needed).

Both security and dependability of the protection system are of paramount importance for reliable and continuous operation and stability of the power system.

The guide starts off discussing general redundancy considerations, thus laying ground for redundancy design options, types of protection system redundancy, and its impact on reliability. It addresses economic, redundancy simplicity, and maintenance aspects that are considered in choosing redundancy design.

The guide analyzes how each component of the protection system affects protection system redundancy. It discusses the impact of two relay systems mounted on separate panels vs. two relay systems mounted on a single panel; separate sets of current transformers (CTs) or voltage transformers (VTs) vs. a single set of CTs or VTs for both relay systems; dual vs. single battery/dc source; and dual vs. single breaker trip coil circuitry.

The guide evaluates redundancy aspects in relay systems relative to their hardware, firmware, and protective functions and in protection communication channels. Also, it discusses redundancy considerations in local area networks and timing systems.

Additionally, the guide provides examples of achieving redundancy for power system equipment protection to assist users in designing redundant protection schemes. These examples illustrate commonly used redundant protection packages for generators, transformers, buses, transmission lines, etc. They do not limit the users from utilizing other package combinations to achieve redundancy.

The guide also provides a redundancy overview for other protection and control functions such as breaker failure, autoreclosing, and system integrity protection schemes (SIPS).

III. General Redundancy Considerations

A. Overview

The effectiveness of a protection system is a compromise between security and dependability during unwanted conditions in the power system. However, the protection system is also expected to operate correctly for unwanted conditions in the protection system itself, such as a failed device. Redundancy addresses these unwanted conditions in the protection system.

The degree of redundancy applied is based on a mix of protection philosophy, the criticality of an element (e.g., transformer, line, bus, generator, etc.) being protected, and imposed requirements. A protection system may include two redundant protection systems that typically consist of two sets of relays, two sets of ac input and dc trip sources, diverse communication routes, etc.

B. Redundancy fundamentals

Protection system redundancy is the design of relaying, auxiliary equipment, and tripping circuits developed to reduce the possibility that a single component failure would prevent the protection system from sensing and isolating a fault in its zone of protection. Protection system redundancy may also reduce the possibility of security loss due to a single component failure.

The zones of protection need to be identified and understood to determine the level of redundancy. Fig. 1 is a visualization of these zones of protection at a substation. The assets available for protection are determined by the connected CTs and VTs. Adjacent zones must overlap for complete protection; otherwise, there would be gaps in protection.

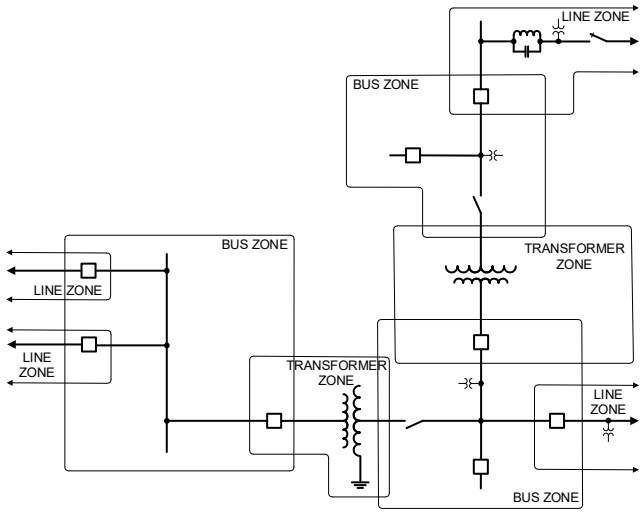

Fig. 1. Zone of protection visualization

Redundancy is applied to protection systems in different ways to improve reliability. Redundant systems do not always have to be of comparable performance.

A redundant system is an additional system that has adequate performance to meet system requirements. A system function that is intended to act only on the loss of another function is considered a backup. The terms “System A/System B” were used in the guide to refer to the redundant protection systems to provide a consistent terminology.

C. Required degree of protection

Depending upon the performance requirements of a system, the following types of protection are applied.

1) Primary

Primary protection operates for each power system element, such as a transformer, in the least amount of time and removes the least amount of equipment necessary to isolate faults located within the zone of that protected element.

2) Local backup

Local backup is applied at the same substation as the primary protection of a power system element. It is intended to operate if the primary protection of the power system element fails. Breaker failure protection that trips adjacent power system elements for a fault in the protected zone is one example of local backup.

3) Remote backup

Remote backup protects a power system element it is assigned to and, additionally, may serve as a backup for a fault occurring in the adjacent zone of protection.

4) Wide area protection

Wide area system protection is used to maintain the reliable operation of the power system for critical contingencies preventing or reducing large-scale power outages.

D. Impact of redundancy on reliability

Redundancy often increases the dependability of an overall protection system since the failure of one protection system would not affect the operation of the other. Generally, an increase in dependability decreases security as additional protection devices increase the risk for an unwanted operation. However, measures to increase dependability may not penalize security to an equal degree.

The guide describes how redundancy influences dependability and security. It illustrates the impact of redundancy on protection system reliability. By adding redundancy to an example system presented in the guide, the probability of a false trip is increased by a factor of 2 while the probability of a missed trip is decreased by a factor of 10,000.

To address the increase in probability of a false trip, a third system can be applied in a voting scheme using a two-out-of-three operation criterion. The guide presents details on how the three systems are connected and the analysis, indicating that the probability of a false trip is greatly reduced while the low probability of a missed trip is maintained. An application of the third system results in improvements in both security and dependability over a single system.

E. Redundancy simplicity considerations

When engineering redundant protection systems, simplicity is a component of a good design. Complicated redundant protection systems and respective controls can be difficult to test or operate. Incomplete understanding of the complexities of these schemes can lead to a human performance error. When setting redundant relays, different elements can be selected for System A and System B relays. However, if there is less experience in applying a protection element to the specific power system, this inexperience may lead to misoperations over time.

F. Other considerations

The guide addresses other considerations when evaluating the level of redundancy to be applied to a protection system. This includes comparing the cost of increased redundancy versus the economic value of power system reliability. The features of relay technologies (electromechanical, solid-state, and microprocessor) and the effect they have on redundancy are discussed. The direct effect of redundancy on availability of the protection system to maintenance is also considered.

IV. Component Effect on Protection System Redundancy

A. Physical redundancy

Physical redundancy, i.e., separating physical location of equipment in a protection system can help eliminate a possibility of single point of failure that could cause the simultaneous failure of two or more complimentary protection systems. While all equipment necessary for a protection system is likely located within the same substation, it may be possible to achieve some separation. For example, cables from the switchyard to the relay panels may be routed by different paths and may help provide continuity of service in case of damage caused by digging or an animal in a cable channel. It is generally easier to accommodate physical separation in new designs than modifying a protection system in an existing substation.

B. Instrument transformer circuits

Instrument transformers typically include voltage transformers (VTs) and current transformers (CTs).

Use of two sets of VTs is an ideal solution; however, this option may be impractical due to space constraints and economic reasons. Typically, VTs have dual secondary windings. Two redundant protection systems can be supplied from separate secondary windings of a given VT. An example of such an arrangement is shown in Fig. 2.

Redundancy in CT circuit can be achieved by utilizing separate CTs for each protection system. An example is shown in Fig. 2, where CTA used for the System A relay is separate from CTB used for the System B relay. The CT currents could be routed using dedicated control cables via different paths to their respective relay systems. Although utilizing dedicated CTs is considered the best practice, it may be acceptable to combine CT circuits for multiple zones of protection based on user's analysis and preference.

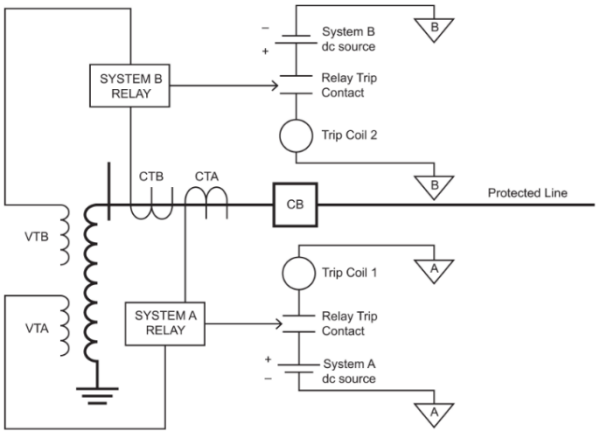

Fig. 2. Dual secondary VT and separated CTs for redundant line protection

The guide also discusses considerations for non-conventional instrument transformers such as optical CTs/VTs, low-power CTs/VTs, Rogowski Coil CTs, and electronic VTs in design of redundant protection systems.

C. Battery/dc/breaker trip coil circuits

For battery/dc source to be considered redundant, a dedicated combination of a battery and a charger with connections for external, mobile, emergency, or temporary operation is used to support the failure of either battery bank. An example is shown in Fig. 3.

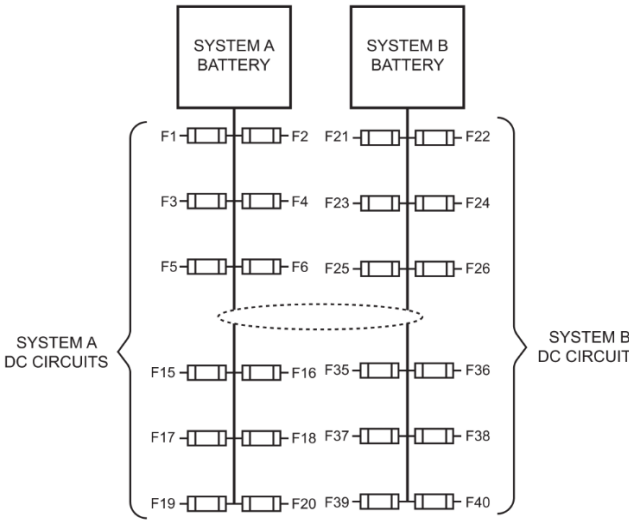

Fig. 3. Dual battery dc circuit method

A dual battery system may be configured such that each battery is large enough to carry the combined load of both System A and System B. A transfer scheme may be implemented to support both systems in case one battery fails. Such level of redundancy is considered the best industry practice, but there may be reasons (such as physical constraints) due to which alternatives might need to be considered. The guide discusses accepted alternative practices, which may also meet regulatory requirements. For example, a non-redundant battery system is monitored and alarmed such that a failure is recognized, and quick mitigating actions are taken.

D. Dc control circuit redundancy

To realize redundancy, a separate dc circuit could be used for each circuit breaker trip coil. The dc circuit associated with protective relaying may be separate from the dc circuits used with the circuit breaker. In this case, a failure of the dc circuit associated with the circuit breaker still allows the protective relay to initiate breaker failure and/or cross tripping. The breaker failure relay may be on its own circuit or use the dc circuit associated with the protective relaying.

E. Breaker trip coil circuit redundancy

In case where a circuit breaker is equipped with more than one trip coil, redundancy is achieved by using an independent dc circuit for each trip coil. When two completely independent protective relay systems are employed, each system can be associated with its own circuit breaker trip coil. This practice may cause an undesirable scenario where breaker trip circuit 1 associated with System A fails and System B associated with breaker trip circuit 2 is concurrently in test or fails so that the breaker may not trip for a fault should it occur at the same time. Another low probability but possible scenario would be where a breaker trip circuit associated with System A is open and System B is slow in operating. Then, an unnecessary breaker failure operation may occur. The guide discusses possible solutions to these problems.

F. Relay systems

Redundant relay systems are self-contained and independent of each other, capable of detecting and isolating faults with dependability and security. Relay systems may be physically separated on a same panel to reduce risk of tripping in-service system during maintenance or testing of out-of-service system. In critical substations, further physical separation of relay systems, i.e., each relay system is mounted on a separate panel, may be used to reduce a risk of complete failure during a catastrophic incident such as a fire. Additionally, the guide considers redundancy improvements from the perspectives of relay hardware, firmware, and protection functions.

1) Hardware

Relay hardware redundancy may be achieved by applying relays from different manufacturers or applying different relay models from a same manufacturer.

Benefits of using different manufacturers for relay systems are as following:

- A component or firmware related failure in one relay system does not affect a relay system by other manufacturer, resulting in at least one relay system available to detect and clear faults.

- Fault detection algorithms are specific to manufacturers. Hence, if the relay system by one manufacturer fails to detect a fault, it is still possible that the relay system by another manufacturer correctly detects and clears a fault.

- Risk of common-mode failure as well as likelihood of common settings error is reduced.

However, factors such as the cost of more complex engineering, design, and maintenance as well as additional training and reduced reliability due to increased likelihood of human error when using different manufacturers also need to be considered.

In case where relay systems by a single manufacturer are preferred, redundancy may be achieved by using two dissimilar models that employ different design, hardware, firmware etc. The design and relay settings may be complicated with this approach; however, using relays from the same manufacturer offers common terminology, setting philosophy and format to ease the development of relay settings as well as commissioning, maintenance, and training. Using identical relays by the same manufacturer offers many advantages such as cost savings in design, setting, commissioning, and maintenance, and it reduces human errors associated with scheme design and relay settings. However, there may be a concern associated with common-mode failure such as possibility of a single problem resulting in failure of both relays at the same time.

The guide also discusses probability assessment of relay hidden failures, typically, discovered after an undesired incident occurs. Refer to guide for further guidance on effect of hidden failures on dependability and security.

2) Firmware

In microprocessor relays, there exists a possibility of software or firmware failures. Relay models by a single manufacturer may share the same protective algorithms found in firmware codes for various protection elements. For example, an overcurrent, distance, or directional element may share a firmware code across the product line offered by a given manufacturer. This practice results in a concern that an error in a firmware code appears in multiple relay models. If two relay systems are used, both employing the same firmware code, the firmware error can cause both relay systems to fail to detect a fault under certain circumstances. To avoid this potential failure, consider using different protection functions. For example, if possible, use a mho distance element in one relay and a quadrilateral element in another relay.

The same common-mode failure concern also applies to communication systems within the relays. Refer to the guide for further guidance and mitigation options.

3) Protection functions

Measures such as using protection functions with different operating principles that complement each other may be applied to achieve redundancy.

For example, line current differential and communication-based distance functions can be used to protect high-voltage transmission lines. The line current differential function can clear a line fault if a VT has failed at one end of the line while the distance protection can operate via a step distance scheme if the communication channel fails. Another example would be to apply high-impedance and percentage-restrained differential schemes to protect a power system bus, thus providing two independent protection methods that complement each other.

The guide also discusses an application of voting schemes when a high degree of certainty, i.e., a relay system would not operate incorrectly, is desired. Such schemes are most utilized in system integrity protection schemes (SIPS) and a few extra high voltage (EHV) transmission line protection applications where system studies or operational experience show that mis-operation or inadvertent loss of transmission poses a risk to overall stability of the system.

4) Control functions

In addition to protection functions, control functions such as automatic reclosing are also discussed. Unlike the protection functions, it is not desirable for both relays to perform the control functions. To address failure of a relay providing a control function, relays could be interconnected (either hardwired or via communication links) to share relay status information. In case the relay providing a control function is disabled, the other relay could be automatically enabled to provide the lost control functionality. However, disadvantages such as extra wiring, more logic programming, extra sequence of event recordings etc. need to be considered when employing this approach.

G. Communications channel redundancy

The guide also discusses protection system redundancy as it pertains to communication channels that are used to exchange protection signals between substations (pilot protection or teleprotection). Redundant communication channels may be used if the loss of the channel may cause undesirable operation. A typical approach is to use independent channels that have both route and technology diversity. A system with one direct fiber communication path and one microwave path is one such example. If one channel fails, the relay system still has a good communication path for protection signals. In the event of a dual-channel failure, the line protection scheme may revert to time-delayed tripping.

1) Power line carrier

Redundancy in power line carrier (PLC) channels can take different forms, providing varying degrees of redundancy. The intuitive solution of coupling one channel to one phase and another channel to another phase may provide redundancy for communication equipment; however, there are isolation issues that can arise from such an arrangement. A better option for PLC channel redundancy is to use center-to-outer-phase coupling. The guide provides more detail and references related to these concerns and solutions.

The highest level of redundancy for a PLC protection channel is three-phase coupling (also called Mode 1 coupling). It utilizes terminal equipment on all three phases and provides more advantages over single-phase or dual-phase coupling. The advantages come at the cost of complexity, however, and the guide discusses these considerations.

2) Multiplexed digital networks

The guide provides several examples of communication channel redundancy using multiplexed digital networks. These networks allow two or more signals to share a common path and provide versatility when it comes to routing those signals. Examples in the guide include point-to-point, ring, and mesh topologies.

The operation of these network types and the implications for protection system redundancy of network failure and switchover time are discussed in the guide. For example, the guide points out that achieving redundancy in point-to-point channels typically requires multiple systems since the loss of one fiber could disrupt multiple protection channels carried on that single path. A separate, redundant point-to-point network operating on another fiber (with route diversity) can be a better redundancy option than redundant terminal equipment operating over a single fiber.

In a ring or mesh network, the failure of any one fiber does not typically cause a loss of the channel since protection signals can be routed in two or more directions and sometimes re-routed. In case of a path failure, the equipment switches to the alternate path. However, there is a failover time associated

with this switching, and that time must be considered by the protection engineer (mesh network failover scenarios can be complex). There also exist failure modes which may cause total failure of the system, which the guide describes before discussing methods of minimizing the risk.

The guide also looks at switched redundancy where two redundant pilot protection channels are connected with AND-logic to decide whether a protection signal is valid. This increases security at the cost of dependability. The guide points out that dependability can be increased with the same scheme by allowing for a switch to single-channel tripping when one channel is lost.

H. Local area network

Moving to networks associated with the newer technologies, the guide then reviews considerations for redundancy in Ethernet LANs carrying protection functions. It discusses the different failure modes associated with these types of networks and steps to mitigate the risk of failure. Redundancy protocols and architecture for Ethernet LANs are covered such as rapid spanning tree protocol (RSTP), parallel redundancy protocol (PRP), and high-availability seamless redundancy (HSR). Block diagrams, overviews, and a comparison between these technologies are provided in the guide.

Like time division multiplexer (TDM)-based networks, Ethernet LANs may be configured with redundant hardware in such a way that no single point of failure can cause a failure of the entire network and, thus, the protection scheme. Network devices can be configured to detect failures and automatically switch over to another path. Data can also be sent in both directions simultaneously, so that a packet is always available in the event one path fails.

As the complexity of Ethernet networks grows, software-defined networks (SDN) can make network management more efficient by de-coupling the management of individual devices from the devices themselves and placing it in a common software control plane. This allows management of an entire fleet of switches via the control plane software itself. The redundant communication paths may be programmed in the control plane as well.

The guide also looks at LAN redundancy considerations for IEC 61850 systems. System A and System B protection packages can be wired for redundancy in these IEC 61850 networks, ensuring that any one hardware failure cannot cause a failure of both System A and System B protection functions.

For IEC 61850 systems, several failure scenarios are given as examples and the network performance in the face of these failures is demonstrated. Methods of mitigating the risk of network failure and increasing communications redundancy are provided such as connecting multiple switches in a ring or providing multiple switches for the System A and System B protection schemes. The benefits of these schemes are described, including the sharing of information between the System A and System B relays.

I. Timing systems

The guide discusses timing systems which are used for local or wide-area time synchronization of analog values and events in power systems. In some cases, timing sources may be unique in redundant protection systems. Where redundant time sources are used, special attention is to be paid to their synchronization and to the cases where they may lose synchronism. An out-of-sync timing source may result in timing errors that can cause adverse effects in protection systems such as misoperations.

V. Redundancy Considerations for Power System Equipment Protection

A failure of a protection system during a fault in a power system could lead to catastrophic events including damage to expensive equipment such as generators and transformers, loss of revenue due to an extended outage, and collateral damage to other equipment in the substation. It could also lead to power outages, power swings, and system collapse due to instability. The guide discusses some of the methods used to achieve protection redundancy for power system elements.

A. Generator

An example of redundant protection systems for a generator is illustrated in Fig. 4. System A provides unit differential protection that includes the generator and its step-up transformer whereas System B provides differential protection only for the generator.

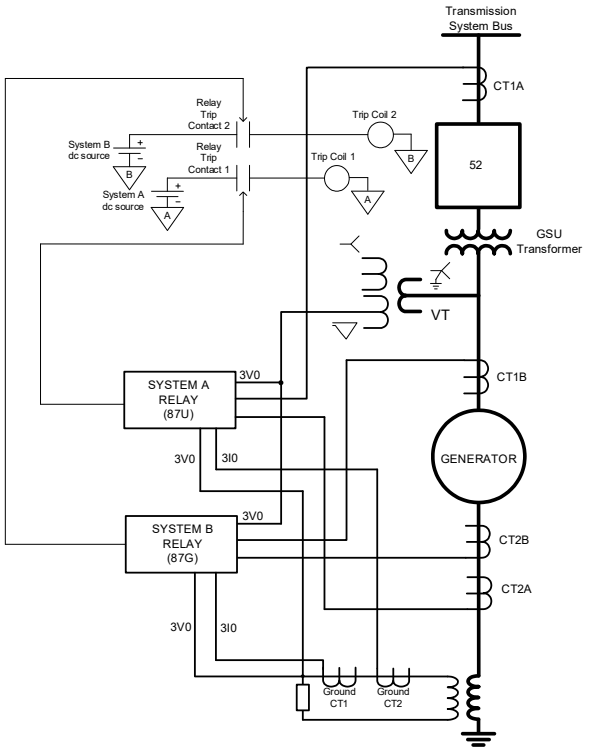

Fig. 4. Generator protection with two relay systems (87U and 87G)

B. Bus

Typical redundant protection for high-voltage and extra high voltage buses can include dual high-impedance differential schemes, dual percentage-restrained differential scheme, or a combination of one of these two schemes. For medium-voltage buses, a transformer differential protection that encompasses the bus and a radial blocking zone-interlock protection with a definite time overcurrent protection are considered redundant.

C. Transmission line

EHV transmission lines are usually a part of a critical path in the power system since they carry the bulk of the load. They are typically protected with redundant protection systems. Fig. 5 shows general redundant protection systems for a transmission line.

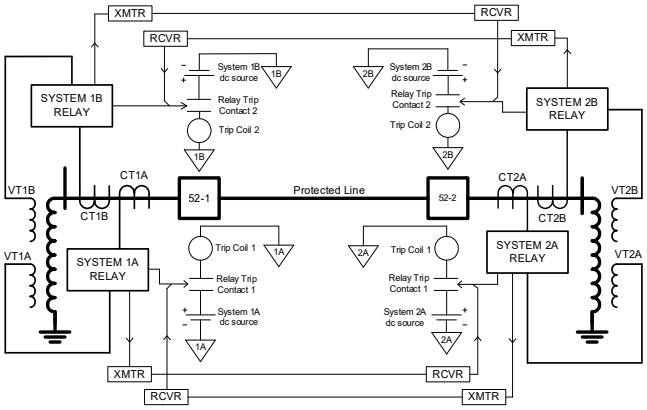

Fig. 5 Redundant line protection example

Depending on the level of redundancy required following aspects are considered:

- Transmission lines that are critical may require redundancy in the communication systems used for teleprotection to maintain fast fault clearing times.

- Critical transmission line relays may not share a common mode failure. For example, a blocking logic of the System A relay may be incorrectly activated. Therefore, it is beneficial that the System A and System B relays do not use the same algorithm because it can result in a common failure resulting in blocking both protections systems during faults.

- System B can have the same performance as compared to System A or a lesser performance degree according to the needed level of redundancy. The same performance level for both systems is typically used for the EHV transmission lines while the same or lesser level is used for HV transmission lines with only one of the relay systems utilizing a teleprotection scheme.

D. Transformer

Common power transformer protection functions include differential, restricted earth fault, sudden pressure, and overcurrent. Users may apply various combinations of these functions to achieve redundancy.

The size of the transformer (MVA) is one of aspects to select a redundancy level for transformer protection.

To achieve the redundant protection of a generator step-up transformer (GSU), some users apply a set of dedicated transformer differential relays and a unit differential relay whose protective zone includes the generator and GSU.

E. Shunt reactor

Protection for EHV shunt reactor units is typically redundant with separate dc supplies, dual trip coils, and separate CT secondary windings. A single protection function with the transformer protection as a backup may be typically provided for lower voltage dry-type reactors connected to a tertiary bus of a transformer. For dry-type reactors, redundant time overcurrent relays are used for multi-phase faults. The transformer bank differential protection would also include

these reactors. In addition, redundant negative sequence protection could be used as a backup. For oil-immersed reactors that are tapped on a line, the line relays provide coverage for phase-to-phase and phase-to-ground faults. The reactors may also have their own protection that trips the transmission line breakers.

F. Capacitor bank

Redundant protection is typically not applied for distribution level capacitor banks. For transmission system capacitor banks, redundant overcurrent schemes using separate CT sets may be applied to mitigate system stability threats arising from short circuits within the capacitor bank protected zone. On the other hand, dual overvoltage and unbalance protection functions are typically not applied since these conditions do not impact system stability.

G. Autoreclosing

Redundancy of autoreclosing is commonly unnecessary because it is a control function and failure to reclose is backed up by local and/or remote manual close.

H. Breaker failure

A breaker failure protective function is provided for redundancy in lieu of using multiple circuit breakers. If this function detects that the circuit breaker has failed to interrupt a fault in its protective zone, it trips adjacent breakers to clear the fault. The security of the breaker failure function is very important.

Maintaining independence between the fault detection and the breaker failure functions with respect to input signals, hosting relays, and tripping outputs may be beneficial for redundancy. To accomplish this independence, the use of a dedicated breaker failure relay may be warranted, in addition to a different CT set and signal paths.

Breaker failure protection can also be integrated in a multifunctional relay that protects a power system element, e.g., a line or a transformer. This eliminates the need for a dedicated third relay, thus reducing cost and needed physical space and wiring, and increases operational flexibility. There are some issues associated with this scheme. One is the added complexity. There is a probability of misoperation if there are redundant breaker failure protection elements for a given fault detection function. If breaker failure is implemented within redundant relay systems, the main fault detection functions are biased towards dependability while breaker failure trip is normally biased towards security. The users need to evaluate the tradeoffs between dependability and security.

I. Distribution systems

The redundancy implementation in distribution protection may be less common than in transmission because the failure of an individual protection component affects fewer customers. The use of redundant protection may be needed for some critical distribution loads. Additionally, the distribution systems have been evolving due to penetration of renewable energy resources, microgrids, and on-site generation. This may require re-evaluation of protection system redundancy in the future.

J. SIPS

System integrity protection schemes (SIPS) usually have redundancy implemented in their design, but this may reduce security. A two-out-of-three voting scheme may be applied to maintain security and achieve dependability of each system; however, this adds complexity.

Mixed use redundant systems include SCADA, SIPS, and protection systems. While the SIPS and protection systems are typically redundant, the SCADA systems may not be redundant. When there is a disagreement in a mixed redundant system, the data can be reconciled between soliciting systems in the separate SIPS systems. Unlike the separate SIPS-relay system, the separate substation SCADA-relay systems can reconcile the data at the local substation SCADA level and the control center level because SCADA provides user-interface functions at both levels.

VI. SUMMARY

The 2021 IEEE C37.120 Guide for Protection System Redundancy for Power System Reliability presents practical solutions to achieving protection system redundancy that helps facilitate the reliable protection response to power system faults and other abnormal conditions.

The guide was developed to aid protection engineers in designing redundant protection systems that are based on the best industry practices and applications and improve protection system dependability and security.