Enhancing Data Center Resiliency: Industrial FLISR for Improved System Fault Management and Availability

Ceeman Vellaithurai, Nate DeBruno, and Tanushri Doshi
Schweitzer Engineering Laboratories, Inc.

Presented at the
52nd Annual Western Protective Relay Conference
Spokane, Washington
October 28–30, 2025

Enhancing Data Center Resiliency: Industrial FLISR for Improved System Fault Management and Availability

Ceeman Vellaithurai, Nate DeBruno, and Tanushri Doshi, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—Data center power delivery systems are built with multiple levels of redundancy to minimize downtime. The medium-voltage (MV) system often features redundant feeds from entirely separate power sources, featuring ring main units (RMU) using breakers or vacuum fault interrupters in loops as a common topology. An industrial fault location, isolation, and service restoration (FLISR) in looped power systems offers a robust and fast approach to detecting faults, enhancing system reliability, and improving service availability while achieving significant cost savings. This scheme leverages the flexible programming platforms of modern intelligent electronic devices (IEDs) used for protection and control to enhance operational efficiency, reduce the number of backup generators that come online, and improve overall system resilience. This system is paired with an event data collection system to provide operators with all required information for faster incident response. This paper includes a discussion of the different data center power system topologies that are typically used and presents two ways of implementing the industrial FLISR system: a localized approach with IEDs using information from only the neighboring devices in the loop to make decisions, and a second approach using a centralized controller to consolidate information and make decisions. Hardware-in-the loop (HIL) simulation is used to show the performance of the system and highlight key benefits.**

In conventional power systems, faults often lead to prolonged outages, requiring backup generators to operate for extended periods to maintain service continuity. Because the proposed scheme enables faster fault detection and isolation by using protection and automation devices with embedded intelligence, restoration is achieved more efficiently, thereby minimizing the number of backup generators that must operate. This results in significant fuel cost savings, reduced wear and tear on generators, and lower maintenance costs. Additionally, by decreasing dependency on backup power sources, data centers can optimize their generation resources and reduce emissions associated with fossil fuel-based backup generation. Reliability and availability improvements are another key benefit of the industrial FLISR scheme. By enabling rapid and automated decision-making at the relay and controller level, service restoration times are significantly reduced, leading to an overall improvement in system reliability. Unlike traditional methods that may require operator intervention and manual troubleshooting of the issue, the proposed scheme enables seamless reconfiguration of the network by rerouting power through alternate paths in the looped system thereby reducing downtime and maximizing the availability of the data center operations.

An HIL simulation setup provides a highly flexible and interactive platform for power system testing and operator training. The HIL setup allows for the simulation of power systems and provides accurate and detailed representations of the power grid, protection systems, and control strategies. Physical devices such as relays and controllers interact with the simulated power grid. Data center operators can benefit from a training perspective through exposure to realistic grid scenarios involving fault and disturbance response. Additionally, this allows for validation and debugging of the developed schemes, which shortens the timeline for field testing and commissioning of these systems.

I. Introduction

Data centers are mission-critical infrastructures that demand exceptionally high levels of power system reliability, availability, and safety to ensure uninterrupted operation. As digital services proliferate and latency-sensitive applications become more prevalent, tolerance for downtime has significantly diminished. To standardize expectations around infrastructure resilience, the Uptime Institute classifies data centers into four tiers: Tier I through Tier IV, as shown in Table I [1]. The classifications are based on the ability of the data center to sustain operations during faults and maintenance events. Tier I facilities offer minimal redundancy, while Tier IV systems are designed for concurrent maintainability and fault tolerance, capable of withstanding multiple simultaneous failures without service disruption.

TABLE I
POWER SYSTEM REDUNDANCY AND TIER ALIGNMENT

Redundancy Model	Description	Failure Tolerance	Tier Alignment
N	Exactly the required capacity to support the load.	No tolerance. Any failure causes downtime.	Tier I
N+1	One additional unit beyond the required capacity.	Tolerates a single component failure.	Tier II/ Tier III
2N	Two independent systems, each capable of supporting full load.	Full fault tolerance. One system can fail.	Tier IV
2N+1	Two independent systems plus an extra spare unit.	Tolerates multiple failures.	Tier IV & beyond/ultra-critical environments

Achieving high-tier compliance requires robust and redundant power delivery architectures, particularly at the medium-voltage (MV) level. These systems often employ looped topologies with dual feeds enabling flexible power routing and fault isolation. Intelligent electronic devices (IEDs)

embedded within these networks provide real-time protection and control capabilities, facilitating automated fault location, isolation, and service restoration (FLISR). When implemented effectively, these systems enhance reliability, reduce downtime, and minimize reliance on fossil fuel backup generators.

In addition to reliability and availability, operational safety is a critical consideration for design. Faults in MV systems pose significant risks to personnel and equipment if not promptly and accurately addressed. Manual operation of breakers, switches, and other power system equipment further exposes personnel to electrical hazards. Modern protection and automation platforms mitigate these risks by enabling rapid fault localization and safe power system network reconfiguration through remote operations.

Despite the benefits of automation, increased system complexity can introduce new risks. According to the Uptime Institute's analysis, human error remains a leading cause of data center outages [2], contributing to over two-thirds of reported incidents. These errors often result from misconfigurations, procedural lapses, or misinterpretation of system behavior. To mitigate these risks, automated systems must be designed with operational simplicity, transparency, and minimal manual intervention. Clear logic flows, intuitive interfaces, and guided workflows are essential to ensure that automation supports, rather than complicates, fault response. These principles guided the authors in the design and implementation of the industrial FLISR system for improved fault management and service availability.

II. Overview of Data Center MV Power System Topologies

The increasing demand for data center uptime and energy efficiency has led to the evolution of MV distribution systems that support high reliability, fault tolerance, and operational flexibility.

Loop-based MV topologies commonly deployed in data centers include the following:

- Disconnects (Fig. 1)
- Vacuum fault interrupters (VFIs) (Fig. 2)
- Ring main units (RMUs) (Fig. 3)

Loop-based MV topologies are preferred because of their inherent redundancy and ability to maintain service continuity during fault conditions. Each unit typically receives power from one side of the loop with sectionalizing performed manually or via motor-operated switches, vacuum interrupters, or breakers. A comparison of features between the three topologies is documented in Table II.

Table II
MV Loop Systems Comparison

Feature	Disconnects & Fused Transformers	VFI	RMU
System Description	Manual loop with load-break disconnects and fused transformers.	Automated loop with pad-mounted switchgear integrating VFIs.	Compact switchgear with breakers and earth switches.
Protection Scheme	Fuses for transformer protection; source breakers for cable and bus faults.	VFIs are deployed to isolate faults with integrated IEDs. Separate zones for cable and bus. Transformers tend to be protected by fused disconnects to save costs. Fast fault clearing is accommodated by communications-assisted schemes.	Breakers are deployed to isolate faults with integrated IEDs. Separate zones for cable, bus, and transformers. Fast fault clearing is accommodated by communications-assisted and differential schemes.
Fault Handling	Source breakers clear all faults. There is no fault discrimination. Manual fault isolation: source breaker clears cable faults.	Fast fault clearing. Use of fuses limits fast acknowledge and reset.	Fast fault clearing time.
Restoration	Typically, manual reconfiguration. If motor operated disconnects and measurements are available, FLISR integration is a possibility. However, because of operation time of disconnects, restoration time will still be slow.	FLISR integration possibility makes restoration faster. However, the closing time of VFIs is typically in the seconds range with values around 2.5 seconds [3]. This limits the restoration time to a moderate value.	Fast recovery via FLISR and automated logic. Fastest possible restoration speed.
Advantages	Low cost, simple design, minimal control complexity.	Automatic fault isolation, remote control, high reliability, and good scalability.	Fastest operation time, fault discrimination, remote control, high reliability, compact footprint, and excellent scalability.
Limitations	Limited automation, limited fault discrimination, high exposure to electrical hazards.	Higher cost, requires additional training for operations and maintenance.	Highest cost, requires skilled configuration, operation, and maintenance.
Best Use Case	Small-scale or budget-constrained facilities.	Tier III/IV data centers requiring high availability and rapid fault recovery.	Mission-critical data centers with space and uptime constraints.

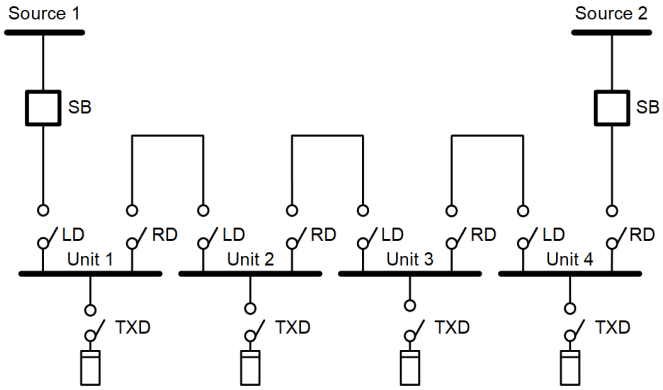

Fig. 1. MV loop architecture with disconnects and fused transformers

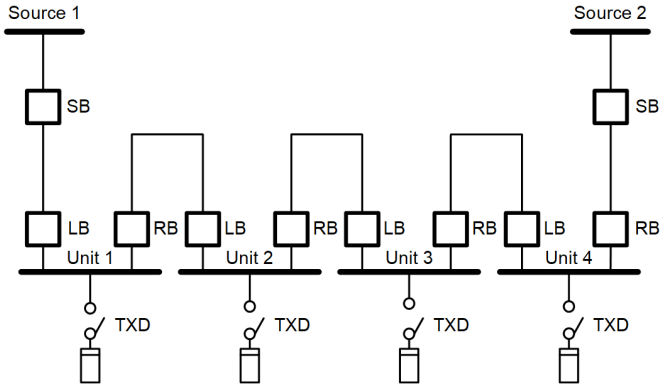

Fig. 2. MV loop architecture with VFIs

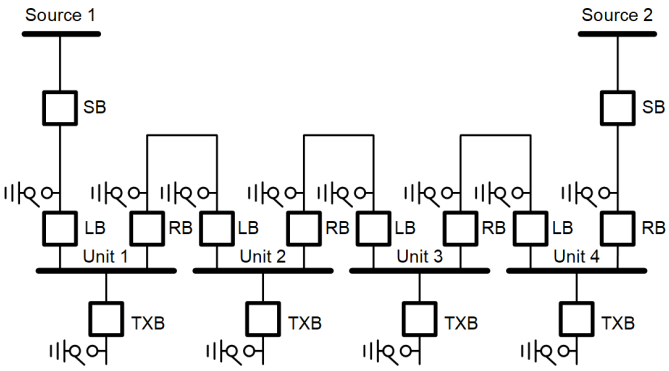

Fig. 3. MV loop architecture with RMUs

III. FLISR Implementation Strategies

FLISR has emerged as a cornerstone of modern distribution automation, particularly in smart grids and mission-critical infrastructures. Recent advancements in distributed FLISR architectures [4] and resilience-oriented restoration strategies have expanded their applicability. However, MV systems in data centers present unique challenges—short cable lengths, high fault currents, and complex looped topologies—that demand tailored solutions. This section examines the implementation of FLISR strategies using the RMU architecture as reference.

A. Centralized Controller-Based Solution

In centralized FLISR architecture, a distribution automation controller performs all fault detection, analysis, and control decisions. Field devices, such as IEDs, transmit operational data to the central controller, which processes the information and issues commands to isolate faults and restore service.

This architecture offers a comprehensive view of the distribution network, enabling the controller to implement optimized restoration, load balancing, and prioritization strategies. However, the scheme relies heavily on the availability and performance of the communication infrastructure. Latency in data transmission and processing can delay fault response, and scalability may become a concern in larger networks.

B. Local IED-Based Solution

Decentralized FLISR systems distribute intelligence across field devices, enabling them to operate autonomously or in coordination with adjacent units. Each IED is capable of detecting faults and executing isolation and restoration actions based on locally programmed logic with information obtained through peer-to-peer communication.

This architecture offers rapid fault response because of localized decision-making and eliminates dependency on centralized control systems. It also enhances system resilience and fault tolerance by allowing distributed operation. However, limited visibility of the broader network can result in suboptimal restoration decisions. Maintaining consistent logic across all devices becomes increasingly complex, especially in meshed or dynamically changing network topologies.

In typical implementations, each relay must receive information about the entire loop to make optimal decisions. This requirement increases configuration complexity, complicates the sequence of operations (SOO), and adds to the operator training and maintenance burden.

C. Hybrid Solution

The hybrid FLISR architecture integrates centralized and decentralized control strategies to capitalize on the strengths of both approaches. This model allocates tasks based on their required operational speeds. Field devices autonomously execute protection-speed tasks such as fault isolation, sectionalizing, and service restoration through peer-to-peer high-speed communication. These devices exchange real-time data and perform rapid switching actions without waiting for central coordination. Fig. 4 shows the hybrid system architecture.

A centralized controller manages automation-speed tasks, including service restoration planning and operator-initiated commands, and a location for concentrating all IED data, Sequence of Events (SOE), alarms, and event data from the system. The controller maintains a global view of the power system network, enabling supervisory control, validation of restoration strategies, and coordination with supervisory control and data acquisition (SCADA) systems.

This dual-layered control strategy ensures that fast-response operations avoid delays caused by communication latency, while still allowing centralized oversight for complex decision-making and operator intervention. It enhances scalability and resilience by distributing intelligence across the network. However, this approach requires a robust and secure communication infrastructure. Additionally, the coordination

logic must maintain consistency between local actions and central policies. This paper builds upon IEEE 2748-2023 [5] and related standards to propose a scalable, hybrid FLISR architecture validated through hardware-in-the-loop (HIL) simulation.

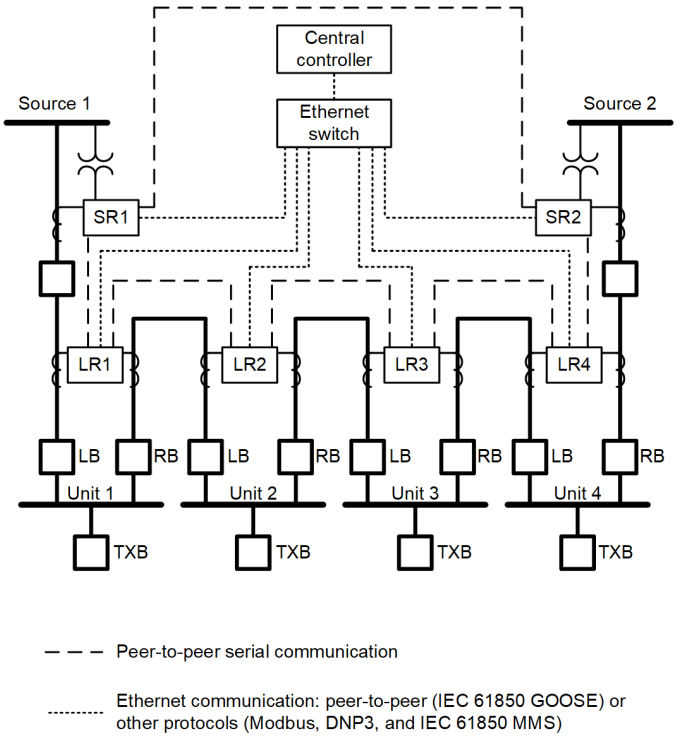

Fig. 4. Hybrid FLISR system implementation

IV. Hybrid System Implementation

The hybrid system architecture is laid out in Fig. 4. The FLISR portion requiring high-speed operation is contained at the relay level between Source Relay 1 (SR1), Source Relay 2 (SR2), Loop Relay 1 (LR1), Loop Relay 2 (LR2), Loop Relay 3 (LR3), and Loop Relay 4 (LR4). Operator-driven reconfiguration, system restore, and other remote operations are performed via the central controller human-machine interface (HMI).

The signals exchanged in the peer-to-peer communication approach, adopting simplicity and allowing scalability of the solution, are depicted in Fig. 5. The exchanged signals are used in protection and control actions.

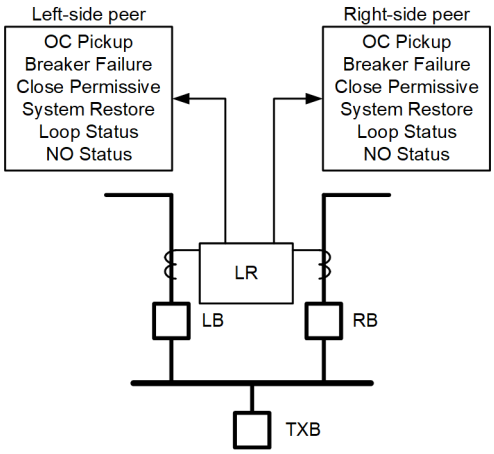

Fig. 5. Signal exchange in peer-to-peer communication

A. *Fault Location and Isolation: Protection System Overview*

The protection system deployed must overcome the following challenges:

- Cable lengths tend to be short with limited impedance leading to fault current levels being similar across the MV system. Fault location discrimination is a challenge.
- Traditional overcurrent element curve stacking with commonly accepted coordination time interval (CTI) will result in very long clearing times. For personnel safety and equipment longevity, it is desired to keep tripping times low.
- Energization of multiple transformers can lead to significant inrush current that may present itself as residual current and elevated phase current. The protection system must not misoperate for this scenario.
- Asymmetrical voltage distribution developed in the network caused by energization of a transformer can cause a form of core saturation, affecting the in-service transformer magnetization characteristics. This phenomenon is called a sympathetic inrush event.

The zone selective interlocking (ZSI) scheme (see Fig. 6) is used in the MV system to enhance fault discrimination and accelerate fault clearing of cable faults [6]. This protection strategy uses communication between IEDs to determine the relative fault location and isolate the affected zone with minimal disruption to the rest of the system. ZSI provides selective and high-speed primary protection for the cable zones, offering a significant improvement over traditional time-coordinated overcurrent protection.

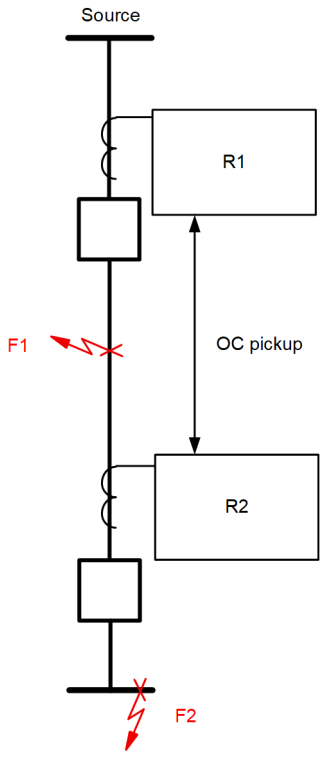

Fig. 6. ZSI scheme operation

Participating relays in the ZSI scheme are configured with sensitive phase and ground directional overcurrent elements. These elements are programmed with short intentional time delays, typically not exceeding 40 milliseconds after element pickup, to allow blocking signals from upstream or downstream relays to be received and processed. This coordination ensures that only the relay closest to the fault operates, preserving service continuity in unaffected zones.

To address current transformer (CT) saturation concerns during high fault currents or simultaneous transformer energization, the scheme incorporates second-harmonic blocking. This technique helps mitigate false residual current readings that could otherwise lead to incorrect ground fault detection, enhancing the reliability of the protection system.

For fault location F1 in Fig. 6, R1 overcurrent element picks up and this is transmitted to R2. R2 does not measure an overcurrent, so R1 does not receive a block. R1 issues a trip command upon expiration of the timer to its breaker. R2 converts the received overcurrent pickup from R1 into a transfer trip and issues a trip command to its breaker. For fault location F2, both R1 and R2 overcurrent elements pick up. Therefore, ZSI tripping logic is blocked from operation in both relays. The protection zones for a four-unit loop are highlighted in Fig. 7.

Combined overcurrent elements are deployed to operate with a preset time delay for faults on the bus, transformer, and cable downstream from within the MV units. Traditional backup overcurrent elements are used to provide backup protection in case of communication failure. The pickup and time delays are determined by site-specific short-circuit protection studies.

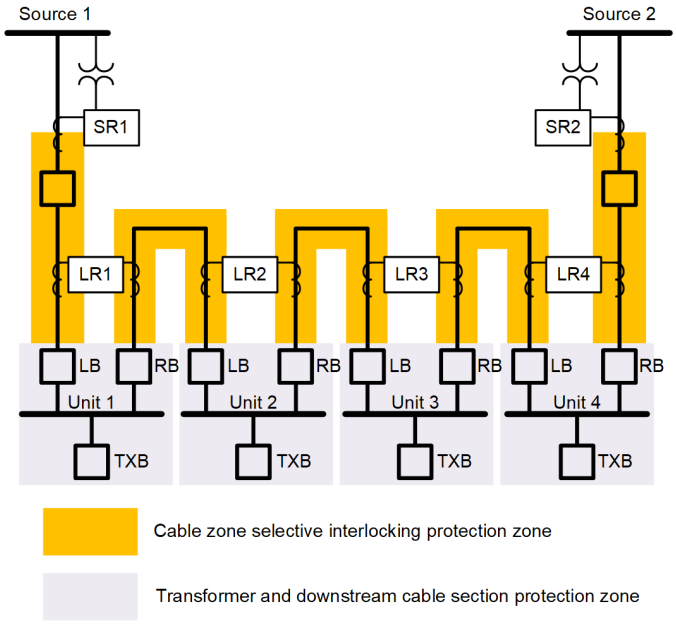

Fig. 7. Defined protection zones

B. *Source Loss and Restoration*

During a source loss scenario, the system is designed to avoid the spinning up of backup power generation resources. Backup generation resources are generally given a 3-second window after an undervoltage condition is detected in the low-voltage (LV) power system before being automatically started. The source loss logic is carefully designed to avoid nuisance tripping, and to ensure that power is restored to all transformers within the 3-second window by transferring any transformers on the dead bus to the live bus. Source loss scenarios are considered within the local IED. Rather than identifying healthy voltage at various legs throughout the power system loop, voltage is only measured at the source bus by SR1 and SR2. These measurements dictate the ability to transfer to the healthy source upon undervoltage detection while load is present. The reliance on only the bus PTs for voltage measurement greatly reduces multiple PT installation and maintenance costs.

Source restoration logic relies on the centralized controller. Source restoration is designed to return the configuration back to the site's normal configuration in an automated fashion. Source restoration begins when the source relay measures that all three voltage phases are above an operator-selectable voltage level. When the source relay reports a healthy voltage to the centralized controller, the centralized controller begins a source stabilization timer; the timer is operator-selectable for the specific site. Once the source stabilization timer expires, the centralized controller automatically issues a system restore signal to open the operator-designated normally open point and close the source relay breaker within the 3-second window to avoid any backup generation starting. In a multiple loop system, each loop is staggered by a calculated preset to minimize the amount of transformer inrush seen at the source.

To improve ease of maintenance, automatic source loss and restoration can be enabled or disabled on a per-loop basis.

C. *Fault Event Management System*

Modern IEDs are capable of capturing voltage and current waveforms using triggers for event capture. Event captures are critical to troubleshooting and resolving fault scenarios quickly. Additionally, the SOE data is recorded in both the IED and controller to document all actions taken by the automated system. A data center can have many of these loops repeated, which greatly increases the number of IEDs. Without an accessible system that is easy to use, understanding a SOO during commissioning or after a fault relies on effective communication with onsite personnel, leading to potentially difficult or inaccurate troubleshooting. This necessitates an automated fault event management using a dedicated system. This system provides a central location for storage and access of events that occur in the system. The information recorded will be used for forensic analysis by engineers and technicians to validate operation of the system.

V. Scenario Walkthrough

The following scenarios describe the working process of the hybrid FLISR implementation.

A. *Scenario 1: Cable Fault*

Fig. 8 illustrates the SOO that occurs upon fault inception. The process unfolds as follows:

1. LR1 detects overcurrent on both CT inputs, Left Breaker (LB) and Right Breaker (RB), indicating a through fault downstream of Unit 1. LR1 transmits the LB pickup signal to its left-side peer, SR1, and the RB pickup signal to its right-side peer, LR2.
2. Both SR1 and LR1 register overcurrent pickup, which restrains the ZSI between them, preventing either relay from initiating a trip.
3. Although LR2 does not detect overcurrent on either CT input, it receives the RB pickup signal from LR1. LR1 does not receive an LB pickup signal, and LR1 and LR2 deduce that the fault lies in the cable section between Unit 1 and Unit 2, based on ZSI logic.
4. LR1 issues a trip command to RB at Unit 1, while LR2 trips LB at Unit 2. Once LR2 confirms the successful opening of LB, it sends a close permissive signal to its right-side peer, LR3.
5. Because Unit 3 LB is configured as the normally open point, LR3 receives the close permissive and commands the breaker to close, thereby restoring power to all units in the loop.

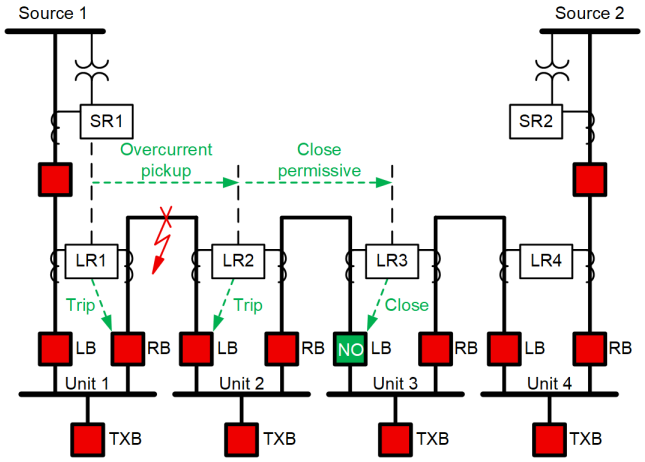

Fig. 8. Scenario 1: cable fault

B. *Scenario 2: Bus Fault*

Fig. 9 illustrates the SOO that occurs upon fault inception. The process unfolds as follows:

1. LR1 detects overcurrent on both CT inputs, LB and RB, indicating a through fault downstream of Unit 1. It transmits the LB pickup signal to its left-side peer, SR1, and the RB pickup signal to its right-side peer, LR2.
2. Both SR1 and LR1 register overcurrent pickup, which restrains the ZSI between them, preventing either relay from initiating a trip.
3. LR2 detects overcurrent on the CT input associated with LB, but not on the RB input. This asymmetry indicates an internal fault within Unit 2, potentially a bus fault, transformer fault, or a fault in the outgoing cable.
4. LR2 issues a trip command to LB and RB. Upon confirming the successful opening of both breakers, LR2 sends a close permissive signal to its right-side peer, LR3. Because Unit 3 is not the normally open point, LR3 forwards the close permissive to LR4.
5. With Unit 4 LB configured as the normally open point, LR4 receives the close permissive and commands the breaker to close, thereby restoring power to all units in the loop.

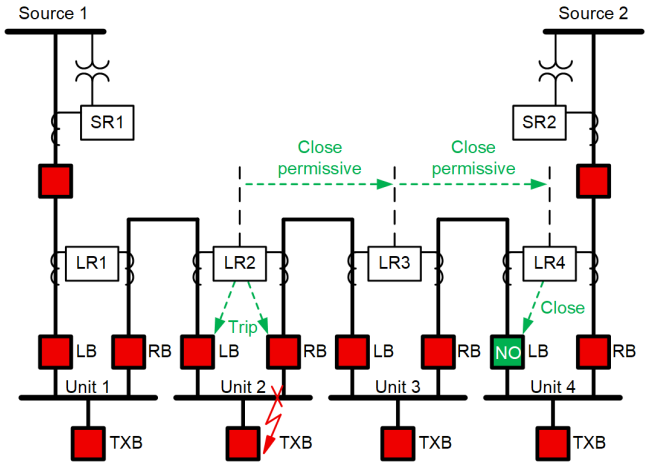

Fig. 9. Scenario 2: bus fault

C. Scenario 3: Loss of Source

Loss-of-source conditions are continuously monitored at Source Buses 1 and 2 by relays SR1 and SR2, respectively. A loss of source is declared when both voltage and current measurements fall below predefined thresholds for a user-defined duration. The SOO following a loss of Source 1 is illustrated in Fig. 10:

1. SR1 detects a loss-of-source condition and commands the breaker at Source 1 to open.
2. After confirming the successful opening of the breaker, SR1 issues a close permissive signal to its right-side peer, LR1. This signal propagates sequentially through LR2 and reaches LR3, which is configured as the normally open unit.
3. LR3 receives the close permissive and commands the normally open breaker to close, thereby restoring power to all units in the loop.

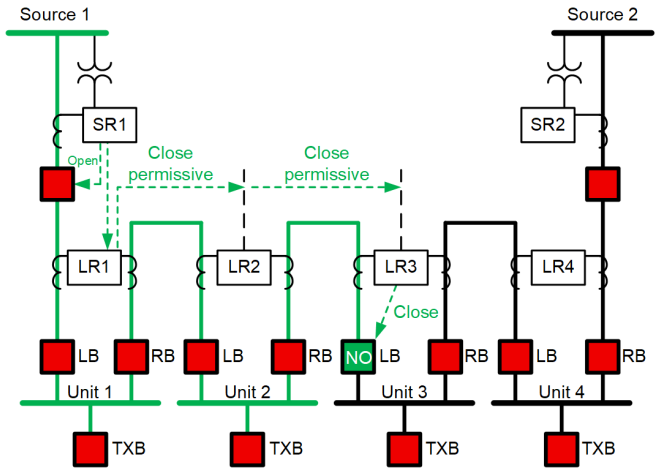

Fig. 10. Scenario 3: loss of source 1

D. Scenario 4: Bus Fault With Communication Failure

Fig. 11 illustrates the fault location in a configuration where the normally open breaker is at Unit 4 LB. In this scenario, peer-to-peer communication between Unit 1 and Unit 2 fails. The reliability of the developed scheme can be viewed in this scenario.

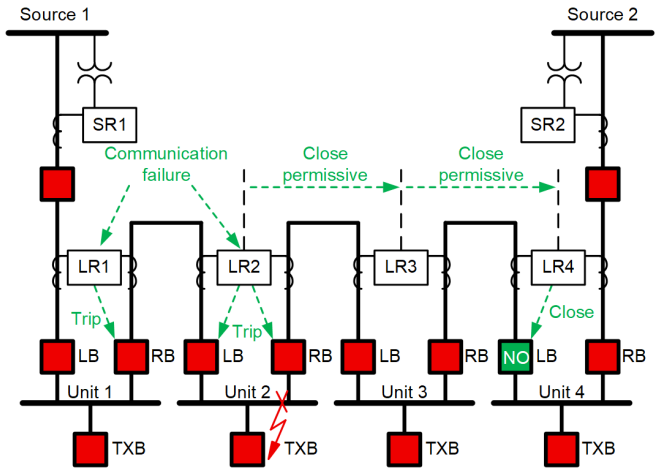

Fig. 11. Scenario 4: bus fault with peer-to-peer communication failure

The SOO proceeds as follows:

1. LR1 detects overcurrent on both CT inputs, LB and RB, indicating a through fault downstream of Unit 1. It transmits the LB pickup signal to its left-side peer, SR1, and the RB pickup signal to its right-side peer, LR2.
2. Both SR1 and LR1 register overcurrent pickup, which restrains the ZSI between them, preventing either relay from initiating a trip.
3. LR2 detects overcurrent on the CT input associated with LB, but not on the RB input. This asymmetry indicates an internal fault within Unit 2—either a bus fault or a fault in the outgoing cable.
4. LR2 issues a trip command to breakers LB and RB. Because of the communication failure, LR1 does not receive the LB pickup signal from LR2 and independently issues a trip command to RB.
5. After confirming the successful opening of LB and RB, LR2 sends a close permissive signal to its right-side peer, LR3. Because Unit 3 is not the normally open point, LR3 forwards the permissive signal to LR4.
6. With Unit 4 LB configured as the normally open point, LR4 receives the close permissive and commands the breaker to close, thereby restoring power to all units in the loop.

E. Scenario 5: Breaker Failure

In Scenario 1, if RB fails to open when commanded by LR1, the system initiates a breaker failure response.

1. LR1 detects the failure of RB to open and issues a breaker failure trip signal to LR2. LR1 trips LB ensuring fault isolation despite the breaker malfunction and declares a “breaker failed to open” alarm for RB.
2. LR2 processes the breaker failure trip, but because LB tripped to isolate the fault based on the description in Scenario 1, the breaker failure signal is discarded by LR2.
3. The breaker failure alarm flags the issue with the breaker and calls for an operator intervention to investigate.

F. Scenario 6: Maintenance

To isolate one or more transformers for maintenance, the operator uses the “transfer” function. The procedure proceeds as follows:

1. The operator places each IED under maintenance into local mode to ensure the IED ignores any open or close command external to the IED.
2. The operator sends an open command to the required breakers to isolate the section scheduled for maintenance.
3. Once in local mode, the operator can be confident that the breakers will not automatically open or close from the SCADA system or the industrial FLISR scheme, ensuring safe isolation while servicing the system.

4. Once the work is completed, the system can be easily returned to normal configuration (see Scenario 7).
5. To improve reliability, local mode is always an alarm in the centralized controller to make sure the device is not left in a local state after work is completed.

G. Scenario 7: System Restore

This scenario begins at the conclusion of Scenario 2. The operator has verified fault clearance, completed inspections and maintenance, reset breaker lockouts, and prepared Unit 2 for reintegration. To restore the system to normal operation, the operator initiates the system restore function via the central controller. The SOO, illustrated in Fig. 12, proceeds as follows:

1. LR3 opens the normally closed breaker in the loop, provided all permissive conditions are met. It then issues a close permissive signal to its left-side peer, LR2, to close the open breakers.
2. Upon receiving the close permissive, LR2 commands LB and RB to close, thereby restoring the loop to its normal operating configuration without the operator issuing three unique commands.

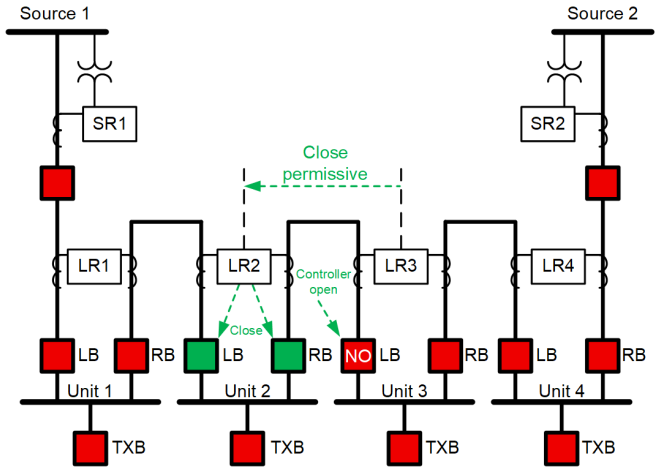

Fig. 12. Scenario 7: system restore initiation by controller

H. Scenario 8: Failure to Open

System restore, as described in Scenario 7, begins with the opening of the designated normally open breaker. This step is critical to reconfiguring the loop for restoration.

If the breaker fails to open during this process, the system raises an alarm to notify the operator. Automatic operation is suspended until the issue is resolved manually, ensuring a safe and controlled restoration.

I. Scenario 9: Failure to Close

As described in Scenario 7, system restore includes a critical step where the normally open breaker must close following a fault or loss-of-source event. If the breaker fails to close after receiving a close permissive signal, the restoration process is interrupted. The system raises an alarm to alert the operator, and automatic operation is suspended until manual intervention resolves the issue. This safeguard ensures controlled recovery and prevents unintended energization.

J. Scenario 10: Anti-Paralleling

Anti-paralleling logic is handled in LR*x* or SR*x* and the central controller.

1. The LR*x* or SR*x* relay issues an open command to the designated normally open breaker.
2. To improve redundancy, if the LR*x* or SR*x* relays cannot successfully open the designated normally open breaker, the central controller issues an open command to the designated normally open breaker after a user-defined timer expires.

VI. HIL Simulation

To validate the performance and reliability of the industrial FLISR scheme presented in this paper, an HIL simulation was conducted using the Real Time Digital Simulator. This testing methodology integrates physical protection and control devices with a simulated power system environment, enabling comprehensive evaluation under realistic operating conditions.

The primary objectives of the RTDS-based HIL testing included:

- Functional validation of the industrial FLISR logic across the various fault scenarios described in Section V.
- Timing analysis of fault detection, isolation, and restoration sequences.
- Verification of peer-to-peer communication between protection and control devices.
- Assessment of system resilience under conditions such as communication failures and breaker malfunction.

Operator proficiency is critical to maintaining data center uptime, particularly during fault conditions and restoration events. The HIL testing platform provides an immersive and realistic training environment, allowing operators to gain hands-on experience with fault scenarios and restoration workflows without impacting live systems.

The HIL simulation environment was designed to support the following operator training goals:

- Familiarization with industrial FLISR logic and its impact on system response.
- Hands-on training in fault diagnosis and response for scenarios such as cable faults, bus faults, and source loss.
- Understanding of restoration sequences and the role of permissive signals.
- Exposure to abnormal conditions, including peer-to-peer communication failures and breaker opening and closing failures.
- Practice in executing manual overrides and system restoration procedures using the HMI.

While RTDS-based HIL testing offers detailed and accurate modeling for engineering validation, additional simulator platforms based on automation controllers complement this approach. The simulator and the IEDs exchange analog and digital data over a selected communication protocol, as shown in Fig. 13. These platforms mimic power system conditions using custom libraries and provide a cost-effective, scalable

solution for operator training across multiple sites. Simplified simulators feature intuitive graphical interfaces and pre-built scenarios, reducing the learning curve for operators.

These simulator-based training platforms do not replace RTDS HIL testing but extend its value by supporting broader training objectives. Once the industrial FLISR logic is validated in RTDS, simplified simulators can be used to train operators on system behavior, alarm interpretation, and manual intervention procedures.

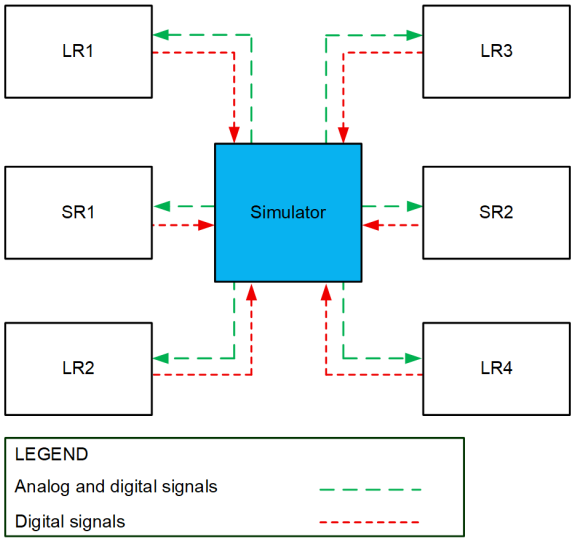

Fig. 13. Signal exchange between the simulator and the relays

VII. Event Report Review

During functional validation and timing analysis using HIL simulation, filtered four samples per cycle event reports were captured for different scenarios. The event capture presented in Fig. 14 is for a three-phase fault at the cable section between SB and the unit 1 LB. The event report provides detailed timing data for a cable fault with the complete sequence of operations included in Scenario 1. Event data from SR1 relay is shown on the left and data from LR1 relay is shown on the right in Fig. 14. The sequence of events with approximate timing information is provided below:

1. 0 ms: SR1 detects a fault condition and transmits the detection signal (SR1_FLT_TX) to LR1.
2. 4 ms: LR1 receives the fault condition detection signal (LR1_FLT_RX) from SR1.
3. 20 ms: SR1 does not receive a fault condition detection signal from LR1 and initiates a trip command (SR1_TRIP) to SB.
4. 28 ms: LR1 does not detect a fault condition locally and initiates a trip command (LR1_TRIP_LB) to the LB.
5. 80 ms: SR1 receives feedback that SB is open (SR1_52A) and transmits a close permissive (SR1_CLPM_TX) to LR1.
6. 84 ms: LR1 receives the close permissive signal from SR1 (LR1_CLPM_RX).
7. 92 ms: LR1 receives feedback that LB is open (LR1_52A_LB).
8. 96 ms: LR1 transmits the close permissive (LR1_CLPM_TX) to LR2 to close the open point in the loop.

The time it takes for LR2 to propagate the close permissive to LR3 is not included in the event report timing diagram. LR3 LB is the open point in this event; it receives the close permissive from LR2 and issues the close command to the LB. The total communication delay to propagate the close command from LR1 to LR3 was between 8 to12 ms.

Based on this analysis, the industrial FLISR isolates the low impedance cable fault and completes service restoration within 100 ms, with much of this time attributed to breaker operation delays.

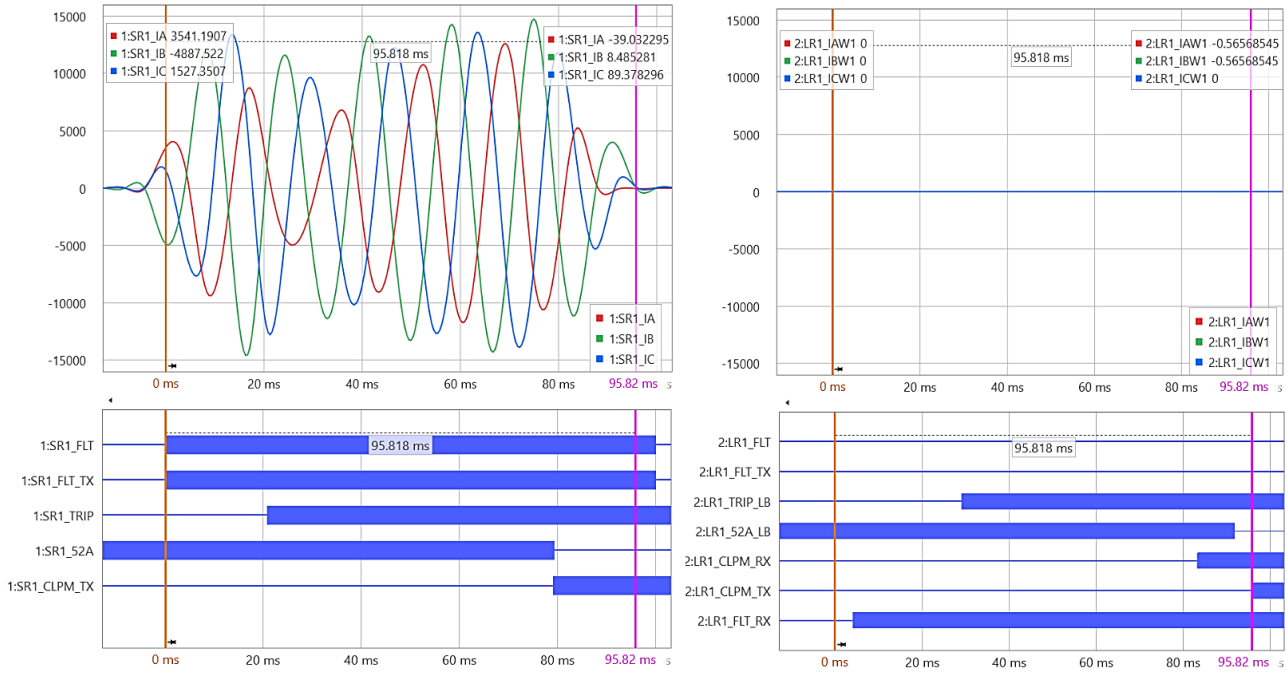

Fig. 14. Event report from SR1 and LR1

VIII. Conclusion

Below are the key features of the implemented industrial FLISR solution:

1. LR*x* IEDs require only current sensing for the scheme to operate.
2. Scalability of the system is unmatched. The communication requirement is limited to the nearest peers in the loop.
3. Arc-flash incident energy levels are kept low using ZSI schemes, improving safety.
4. The system is resilient in the face of communication failures.
5. Simple to operate and maintain.

This paper presents a robust and scalable FLISR strategy tailored for MV looped architecture in data centers. By integrating IEDs with both decentralized and centralized control layers, the proposed hybrid system achieves rapid fault response, minimizes downtime, and enhances operational resilience. The use of high-speed peer-to-peer communication among relays enables protection-speed actions, while centralized oversight supports supervisory control and restoration planning.

ZSI schemes improve fault discrimination and reduce arc-flash energy, contributing to safer operations. The architecture's simplicity, modularity, and reliance on minimal sensing inputs make it highly adaptable to diverse data center configurations. Furthermore, the reduction in backup generator usage during fault events contributes to operational cost savings and environmental benefits. Overall, the proposed FLISR solution offers a practical and future-ready approach to achieving high reliability and availability in mission-critical power systems.

IX. References

[1] Uptime Institute, *Data Center Site Infrastructure Tier Standard: Topology*, Uptime Institute, LLC, 2018. Available: Uptime-Tier-Standard-Topology.pdf.

[2] A. Lawrence, *Outages: Understanding the Human Factor*, Uptime Institute, June 2022. Available: Outages: understanding the human factor - Uptime Institute Blog.

[3] Eaton Corporation, *VFI underground distribution switchgear*, CA285004EN, April 2021.

[4] C. Ruvalcaba and H. T. Le, "Simulation of Smart Fault Location, Isolation, and Service Restoration Scheme with Load Balancing in Distribution Grid," International Journal of Power Systems, vol. 8, no. 2, pp. 10–22, 2023.

[5] IEEE Std 2748-2023, *IEEE Recommended Practice for Fault Diagnosis and Protection in Smart Distribution System*.

[6] T. Doshi, D. Anderson, K. Lythgoe, and K. Sheffler, "Trans-Alaska Pipeline System—Improved Safety and Reliability Via Main-Tie-Main, Arc-Flash, and Fast Bus Protection Schemes Using IEC 61850 Over a Software-Defined Network," proceedings of the 71st Annual IEEE IAS Petroleum and Chemical Industry Technical Conference (PCIC), Orlando, Florida, 2024.

X. Biographies

Ceeman Vellaithurai received his BE degree in electrical and electronics engineering from Anna University Tiruchirappalli, India, and his MS degree in electrical engineering with specialization in power systems from Washington State University. He is currently working in the SEL Engineering Services, Inc. (SEL ES) Data Center Engineering division as an engineering manager. His research interests include real-time modeling and simulation of cyber-power systems. He has authored a patent and several technical papers with over 900 citations. He is a registered professional engineer and a senior member of IEEE.

Nate DeBruno received his BS degree in Electrical Engineering from California Polytechnic State University, San Luis Obispo, California, USA. He currently serves as an engineering manager in the automation specialty at SEL Engineering Services, Inc. (SEL ES). Nate has extensive experience programming and deploying advanced automation schemes in industrial power systems and process control environments.

Tanushri Doshi received her MS degree in electrical engineering from Arizona State University and her BTech in electrical engineering from the Visvesvaraya National Institute of Technology, Nagpur, India. She is currently working in the SEL Engineering Services, Inc. (SEL ES) Data Center Engineering division as an engineering manager. Tanushri has extensive experience in the protection of power delivery systems with a focus on solving challenges as they pertain to safe power distribution and wildfire mitigation. She has designed, developed, and tested protection and control schemes using hardware-in-the-loop simulation environments. She is a registered professional engineer (PE) in the state of Arizona and Montana and a senior IEEE member. Tanushri serves as an associate editor for IEEE IAS PCIC.