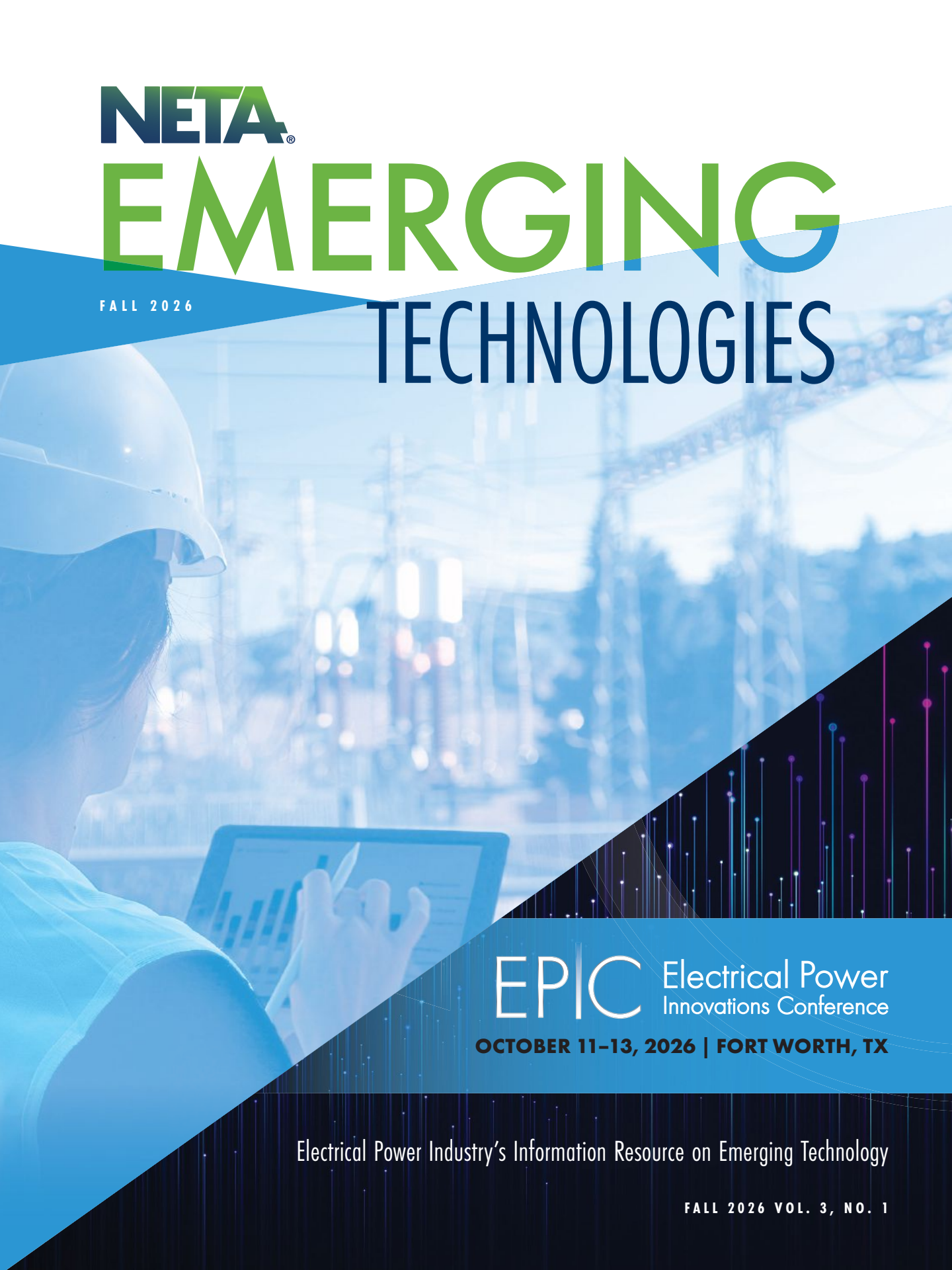
NETA®

EMERGING TECHNOLOGIES

FALL 2026



EPIC Electrical Power Innovations Conference

OCTOBER 11–13, 2026 | FORT WORTH, TX

Electrical Power Industry's Information Resource on Emerging Technology

FALL 2026 VOL. 3, NO. 1

PROGUSA

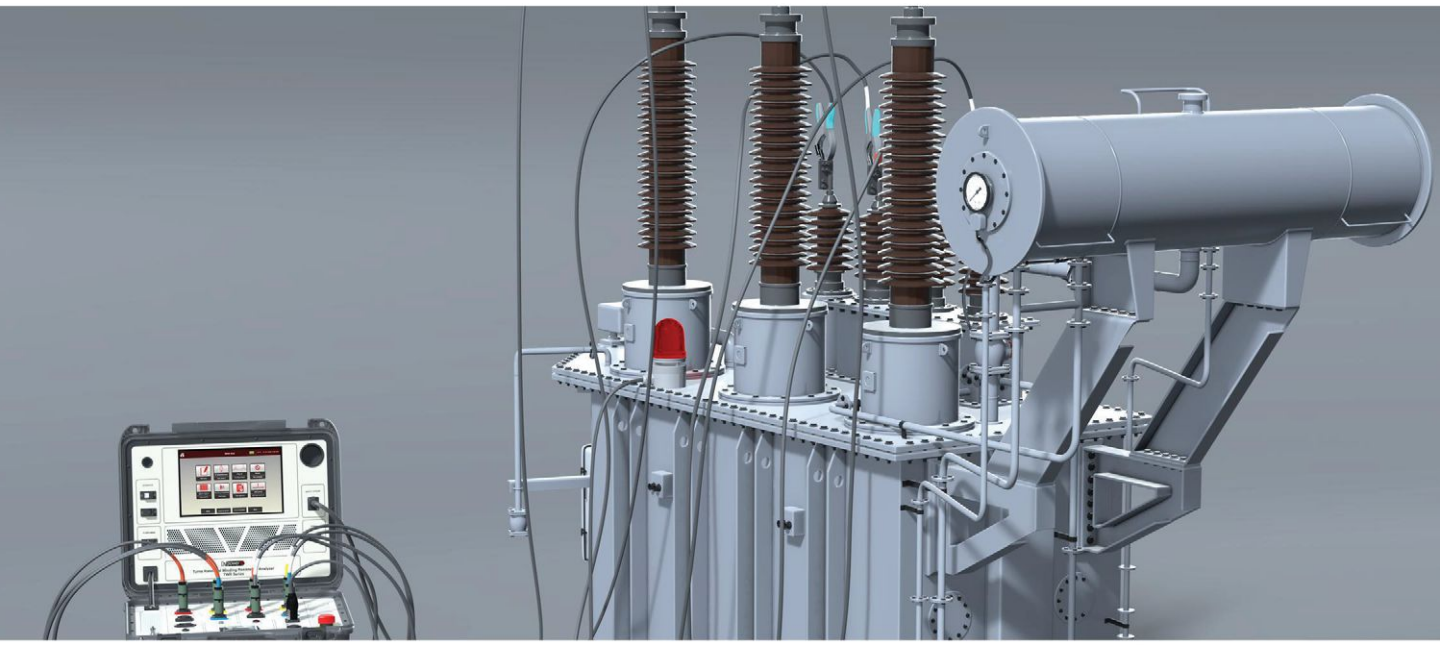
DV power

NEW FOR 2026

TWR250B

Turns Ratio & Winding Resistance Analyzer

ONE-TIME CONNECTION **MULTIPLE TESTS**



Turns Ratio | Winding Resistance | Tap Changer DRM | Demagnetization | Magnetic Balance

- One-time connection to all windings
- 250 V AC turns ratio · 25 A DC test current
- Built-in tap changer control unit
- Battery or mains powered
- 10.1-inch touchscreen, built-in printer
- DV-TR reporting software included

See full specs or book a demo

progusa.net/twr250b

Equipment + Education + Service = Partnership

progusa.net | info@progusa.net | +1 407 332 8678

NETA

EMERGING TECHNOLOGIES

FALL 2026



A *NETA World* journal Special Supplement

News on the latest electrical equipment technology, test equipment innovations, and advancements in electrical infrastructure design.

4 MANAGING, OPERATING, AND OPTIMIZING ELECTRICAL INFRASTRUCTURE IN OIL AND GAS
By Brad Fryrear and Fabio Perea, GERS

10 AN INTRODUCTION TO MICROGRID SYSTEMS
By Tyson Bittrich, Mayfield Renewables

14 ENHANCING CYBERSECURITY IN THE ENERGY GRID: FROM MONITORING TO ENGINEERED RESILIENCE
By Keon McEwen, Black & Veatch

20 DIGITAL SUBSTATION APPLICATION CONCEPTS FOR IBR RENEWABLE ENERGY PLANTS
By Wayne Hartmann, GE Vernova, USA

COVER PHOTO: © STOCK.ADOBE.COM/CONTRIBUTOR/208365358/DAWDUNIA

MANAGING, OPERATING, AND OPTIMIZING ELECTRICAL INFRASTRUCTURE IN OIL AND GAS

BY BRAD FRYREAR AND FABIO PEREA, *GERS*

Oil and gas companies and their associated utilities require strategic geospatial solutions to enhance oversight of electrical infrastructure. Integrating geographic information systems (GIS) with power system analysis software enables real-time asset visibility, improves operational safety, and supports data-driven planning. Industry studies and field implementations have demonstrated significant operational benefits, including reduced data retrieval times, improved maintenance efficiency, and enhanced system reliability. This approach supports compliance with NFPA 70E, *Standard for Electrical Safety in the Workplace,* and IEEE Std. 1584-2018, *IEEE Guide for Performing Arc-Flash Hazard Calculations,* reduces operational risk, and strengthens capital investment decisions—delivering measurable value across large-scale, geographically distributed field operations.

Electrical networks are fundamental to the reliable operation of oil and gas facilities, and effective management of system components is essential for optimizing efficiency across extraction, processing, and distribution processes. As infrastructure expands and becomes more complex, the demand for advanced information management solutions continues to grow.

Modern GIS-based platforms, when integrated with electrical modeling and analysis tools, provide a comprehensive framework for managing these networks. This integration enhances operational visibility, improves system understanding, and enables more informed technical and economic decision-making. Digital transformation initiatives in asset-intensive industries have been shown to significantly improve operational performance and reduce troubleshooting time.

THE VALUE OF INFORMATION

Over the past decade, operational data management has evolved from paper-based documentation to integrated digital systems. This transformation enables advanced data acquisition, storage, and analytics, improving operational efficiency and insight.

Effective systems must ensure:

- Adequate data availability
- High accuracy and timeliness
- Rapid accessibility

Structured data management supports a comprehensive, digitized inventory of electrical infrastructure, including medium- and low-voltage systems and associated process equipment. In current advanced internet architecture, cybersecurity and real-time information access are essential because

data center infrastructure and data science algorithms increasingly govern data integrity, availability, operational insight, and secure decision-making across distributed industrial environments.

OPERATIONAL OPTIMIZATION

An organized and accessible database supports multiple operational functions:

1. **Electrical system operations.** Field-validated models with the individual geographical information of the components enable simulation under normal and contingency conditions, improving reliability and reducing unplanned outages. The geospatial component allows the operators of the electrical system to make decisions regarding the efficiency of the troubleshooting and improve the response times, as the position of the assets is displayed on satellite imagery maps.

2. **Planning and investment.** Accurate asset data, enriched with truthful information captured from the field, improves expansion and upgrade planning by enabling more efficient capital allocation. When the database is comprehensive, precise, and geolocated, planning projects are managed on a reliable basis because the number of assumptions becomes negligible. Asset management is also optimized because the data collection process records each asset's condition, age, nameplate information, and other relevant details, along with attached photographs that support validation, maintenance prioritization, and long-term investment decisions.

3. **Equipment and personnel protection.** System modeling of electrical components worldwide supports protection coordination because the protective devices are captured with high-resolution pictures, allowing the engineering team to utilize the real type, model, manufacturer, and time-current characteristics for an accurate estimation of fault-clearing times and selective device coordination. In addition, a reliable arc flash analysis in accordance with NFPA 70E and IEEE 1584 improves worker safety.

Figure 1 shows how the previous functions interact to provide the final user with fast, straightforward, and effective access to a comprehensive overview of their entire electrical infrastructure.

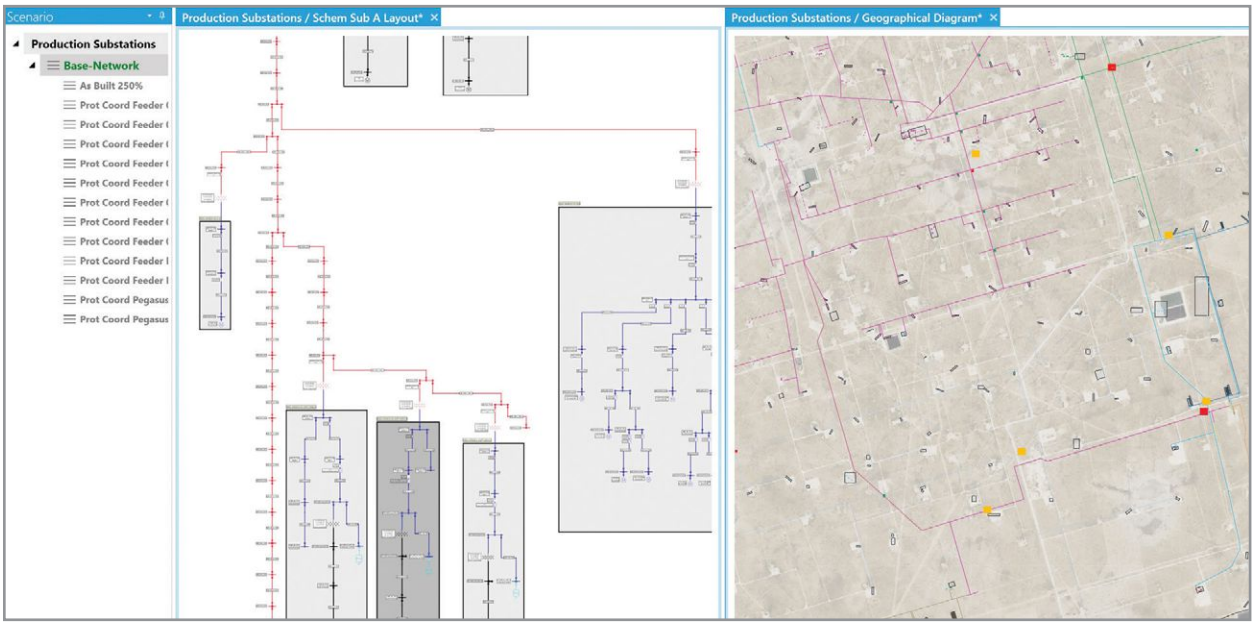


Figure 1: *Geo-Schematic Simulation Database*

IMPLEMENTATION METHODOLOGY

A typical implementation of electrical system inventory and geo-modeling for engineering analysis and asset management includes a structured sequence of activities intended to transform dispersed field information into a verified, geolocated, and analytically useful database:

1. **Geographical engineering database design.** Customized attributes, standardized equipment forms, hierarchical asset relationships, and display icons are defined for each electrical component to collect information under a consistent technical structure.

2. **Field data acquisition, validation, and mobile data collection.** Qualified technicians conduct site visits using mobile applications to record attributes defined in the database design, including location, nameplate data, equipment condition, age, installation characteristics, and photographic evidence to support subsequent engineering review.

3. **Data processing and standardization.** The information collected in the field is synchronized to a controlled cloud environment, where completeness checks, spatial verification, and technical quality control can be performed before the records are accepted as part of the authoritative asset inventory. Engineering personnel review the collected information, standardize naming conventions, resolve inconsistencies, and provide feedback to field crews, thereby refining the collection process and improving the reliability of the final database.

4. **Integration with analysis software.** The validated geospatial database is migrated or linked to a compatible power systems calculation engine, allowing the same asset records to support load-flow, short-circuit, protection coordination, arc flash, harmonics, reliability, motor-starting, and network optimization studies. This is developed from a consistent data foundation, reducing duplicated effort and improving the traceability of assumptions, calculations, and recommendations.

An illustration of the process is displayed in Figure 2.

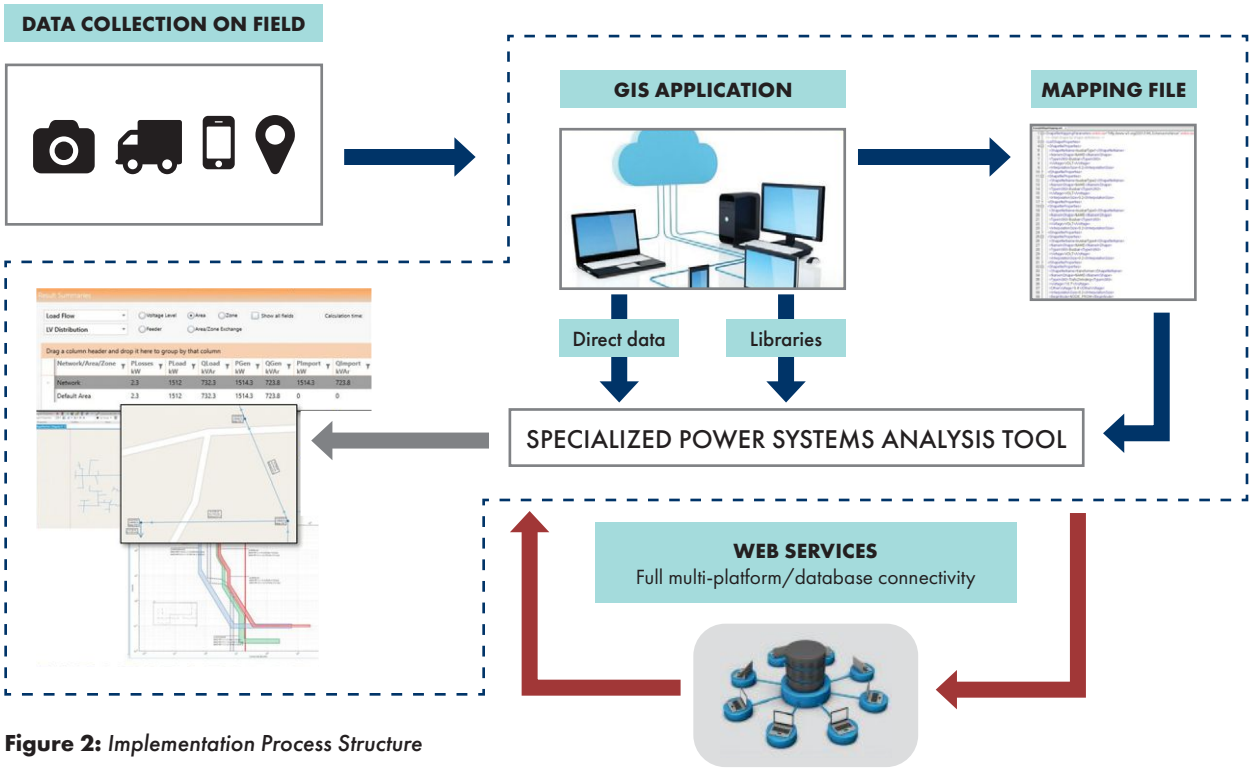


Figure 2: *Implementation Process Structure*

INDUSTRY APPLICATION

Considering that a geographical database can be extended to more than 2,000 gigabytes, the described methodology can cover data ranging from small individual facilities to complex, widespread sets of oil and gas fields. A real case within the Texas industry demonstrates the scalability of the asset management optimization techniques and digitalization for managing complex electrical systems in geographically dispersed operations. Using the number of devices of multiple geographical databases and safety compliance summarized in Table 1, Figure 3 shows the extent of a sample section of the mentioned application.

OPERATIONAL BENEFITS

A structured asset mapping and management approach, along with digital data availability, provides the following operational advantages:

- Geospatial visualization of assets for accurate decisions considering the field's real constraints
- Detailed equipment data recording, which allows the user to verify the condition of the equipment
- Centralized GIS database accessible for every stakeholder
- Integration with electrical analysis tools, providing a multi-analysis option
- Asset classification and reporting, which appropriately creates and tracks its lifecycle
- Arc flash labeling for a safe workplace and regulatory compliance (OSHA/NFPA 70E/IEEE 1584)
- One-line diagrams with simulation results that support the engineering analysis

Collectively, these benefits demonstrate how integrated geospatial asset management improves visibility, data accessibility, analytical consistency, safety compliance, and operational efficiency across electrical infrastructure.

The exposed methodology remains compatible with cybersecurity policies because the final user can determine whether the database is allocated within its own protected servers or hosted in the cloud GIS platform, according to internal governance, access control, and information security requirements.

Artificial intelligence further amplifies these benefits by converting complete electrical equipment

Table 1: *Representative Asset Inventory*

Item	Quantity
Primary/secondary poles	64,280
Motors	13,970
Transformers	18,120
Line length (miles)	2,654
Images collected	416,110
Arc flash labels installed	>30,000
Area covered (acres)	15,234,470

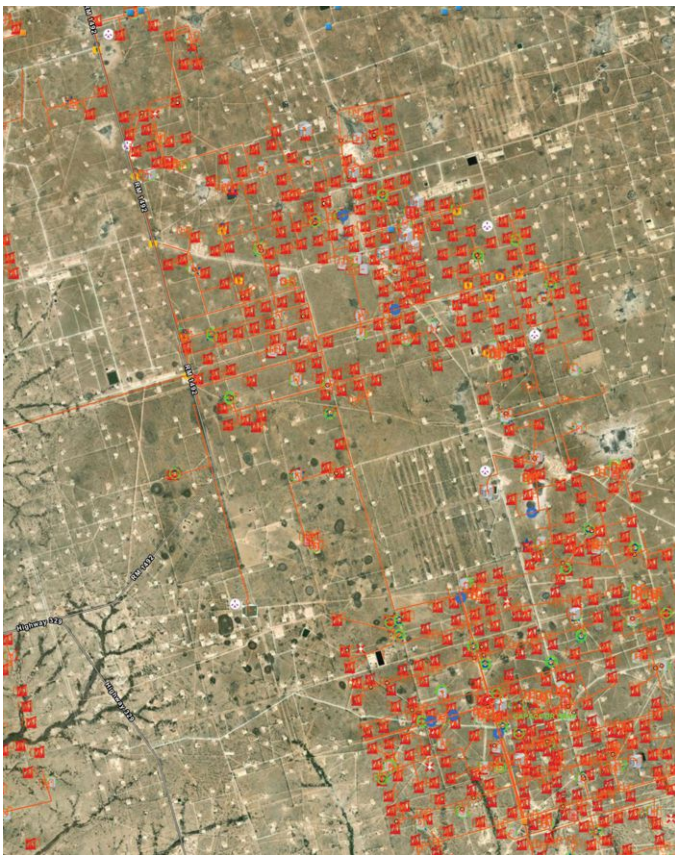


Figure 3: *Texas Case Study Sample*

inventory, associated photographs, cloud-accessible records, and geographical stamps into actionable intelligence. Machine learning and computer vision can support anomaly detection, automated data validation, predictive maintenance prioritization, and contextual decision-making, thereby increasing reliability, traceability, and operational value across widespread distributed assets.

CONCLUSION

Integrating geographically based asset management with electrical power system modeling provides a rigorous framework for managing any kind of industry, as shown for the oil and gas electrical infrastructure. By combining geolocated field data, validated equipment information, and analytical simulation capabilities, this approach enhances safety, reliability, planning accuracy, and operational efficiency, while supporting informed capital investment decisions and long-term asset optimization across geographically dispersed facilities. ■

REFERENCES

[1] ESRI. *Modernizing Asset Management-Electric and Gas Utilities.* eBook. *www.esri.com/content/dam/esrisites/en-us/media/ebooks/electric-asset-management-ebook.pdf.*

[2] Buck, C., Clarke, J., et al. "Digital transformation in asset-intensive organizations: The light and the dark side, *Journal of Innovation & Knowledge* 8 (2023): DOI:10.1016/j.jik.2023.100335.

[3] Deloitte. "Digital transformation in oil and gas companies," blog, *www.deloitte.com/us/en/services/consulting/articles/digital-transformation-in-oil-and-gas.html.*

[4] EPRI. Condition-Based Maintenance Guideline: Including Startup and Shutdown Monitoring. 2022. *www.epri.com/research/products/000000003002023778.*

[5] NFPA 70E, *Standard for Electrical Safety in the Workplace,* 2024 Edition.

[6] IEEE Std. 1584-2018, *IEEE Guide for Performing Arc-Flash Hazard Calculations.*

[7] IEEE Std. 3007.2-2010, *IEEE Recommended Practice for the Maintenance of Industrial and Commercial Power Systems.*



BRAD FRYREAR *is an NFPA Certified Electrical Safety Compliance Professional for GERS, specializing in arc flash risk assessments, power system studies, and utility asset management. His work focuses on leveraging modern technologies, including GIS, to improve the accuracy, efficiency, and accessibility of electrical system data. He received his BAS from the University of Texas Permian Basin.*



FABIO PEREA *is a NETA Level 3 Certified Technician, an NFPA Certified Electrical Safety Compliance Professional, and a Senior Electrical Engineer at GERS. He works as a power systems consultant specializing in large-scale transmission and distribution planning, geographical information system interfaces, protection coordination, optimization techniques, and arc flash safety studies across the oil and gas, mining, and utility sectors. He received his BS in electrical engineering and a post-graduate degree in transmission and distribution of electrical systems from the University of Valle in Cali, Colombia.*



MORE TESTING. LESS REPORTING.

FieldTestPRO eliminates hours of manual reporting with powerful tools built for electrical testing professionals.

- Cloud Based with Online & Offline Modes
- Historical Results & Issue Tracking
- Generate Professional Reports in Minutes
- Fully Customizable Form Templates
- Handwritten -> Digital (OCR)
- Results Portal for 24x7 Report Access

Ready to save time and work smarter?

SCHEDULE A DEMO TODAY

*Mention promo code **EMERGE** to get 20 hours of free template design.*

FieldTestPRO
a KEYPRESS solution

***THE** modern test reporting platform.*

fieldtestpro.com

AN INTRODUCTION TO MICROGRID SYSTEMS

BY TYSON BITTRICH, *Mayfield Renewables*

Within the commercial and industrial renewable energy sector, few terms have garnered more attention lately than the system label "microgrid." This article provides an overview of microgrid fundamentals: what a microgrid is and what it can do.

WHAT IS A MICROGRID?

The answer depends on who is asking and answering. From our experiences, we'll stipulate that most microgrids share these four features—all within a defined boundary:

1. **Distributed energy resources (DERs).** Local (on-site) energy storage and generation sources can function independently from the centralized, bulk power supply infrastructure.
2. **Islanding capability.** The system is ready to operate independently of the grid and can transition predictably between grid-interactive and islanded modes.
3. **Electrical loads.** The known sets of loads served in grid-interactive and island modes.
4. **Dispatchable energy source.** One or more DER can be dispatched at will to serve the electrical load.

This description may feel too general, nondescript, or incomplete, especially to those who are already actively developing, designing, owning, or operating microgrid systems in the commercial and industrial market space. Let's take a closer look at each in turn.

To elaborate on the DER's condition, hird-party consultants or engineers-of-record predominantly work with the latest inverter-based resources, such as solar photovoltaics, lithium-ion battery energy storage, and generators (Figure 1).

Yet, with an eye for any energy future that includes a diverse abundance of renewable energy solutions, any good microgrid definition should consider proven technologies such as fuel cells, modular nuclear reactors, turbine-based assets, and any number of non-lithium storage technologies, including compressed air, redox flow-battery, thermal systems, pumped hydro, flywheels, and others. Notice that a simpler system consisting of loads, a generator, and proper controls for islanding capabilities could meet this four-part definition of a microgrid. This working definition is intentionally open-ended to accommodate all possible DER combinations.

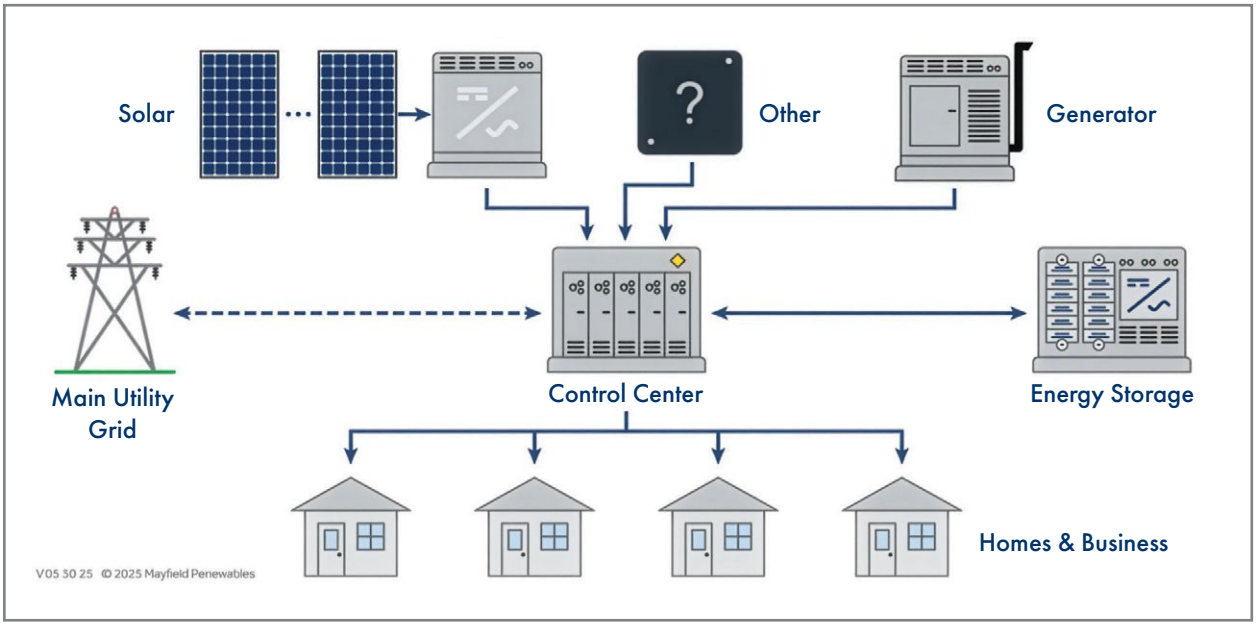


Figure 1: *Microgrids Rely on Various Distributed Energy Resources*

ISLANDING

Some off-grid energy systems in remote areas far from the bulk energy grid demonstrate features 1, 3, and 4, but are not designed for grid interaction and are always islanded. We do not exclude these types of systems from the rest of this article; however, based on our experience, they are more the exception than the rule.

In most cases, the transition from grid-interactive to islanded and back again to grid-interactive is a key feature of microgrid design (Figure 2). However, this transition can present significant design challenges and considerations. Questions may include:

- How quick is the islanding transition?
- Can I avoid having to black-start my motor loads?
- How do I integrate a generator or an uninterruptible power supply (UPS) with a BESS, and which turns on first?
- Who defines and programs the sequence of operations if PV, BESS, and a generator are talking to each other?

BACKUP LOADS: WHICH ONES, HOW MANY, AND FOR HOW LONG?

At the outset of a microgrid feasibility study, it's vital to align expectations among client(s), design team(s), and other stakeholders on load selection and preliminary resilience targets. Optimizing a microgrid design to meet a facility owner or operator's specific resilience targets—whether in hours, days, or weeks—is usually accomplished by a) reducing the amount of load the system needs to serve for some or all of the resilience period; b) increasing energy generation and storage capacity; or c) both. Let's spend a little time looking at load selection.

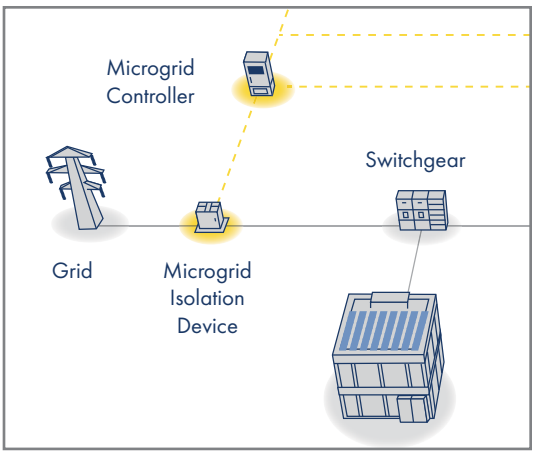


Figure 2: *The ability to island from the grid while continuing to serve on-site electrical loads is important.*

Schemes for managing backup loads can range in complexity. Perhaps you're committed to a full-facility backup, or you are tasked with backing up a whole campus. An example is shown in Figure 3.



Figure 3: *How long a microgrid can supply a load depends on how many loads it's serving.*

In a partial-facility backup design, the loads the facility cannot do without during an outage can be aggregated separately from loads that the facility operator might afford to leave unpowered.

In Figure 4, backup loads are aggregated in two backup load panels that can be isolated from the grid with the inverter bypass switch. During an outage, only the backup loads will receive power from the PV and BESS.

Taking load management one step further in complexity, what if I want to provide full-facility backup for as long as possible but also have the flexibility to remove some loads to extend the resilience period if needed? There could be any number of reasons to reduce load to the most important ones. When the time is right, a microgrid controller, contactors and relays, and subsystem controllers can be programmed and coordinated to shed predetermined sheddable loads in order to keep the most important loads powered. Consider load shedding based on battery state-of-charge (SOC) as one example, shown in Figure 5.

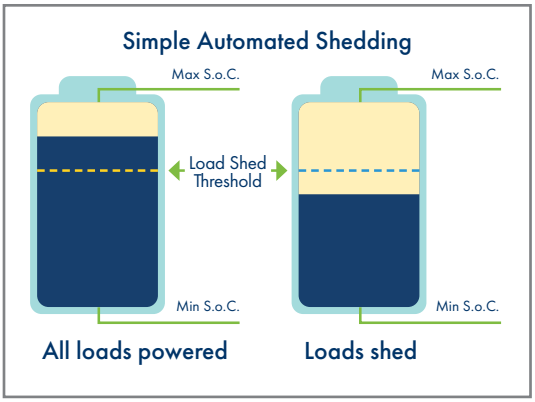


Figure 5: *Simple Automated Shedding*

Within the usable energy capacity of a BESS, an SOC threshold can be designated to initiate load shedding. Here, the microgrid will transition from full-facility backup to partial-facility backup when SOC falls below a programmed threshold.

Here's what programmable load shedding can look like in a single-line diagram (Figure 6). In this case, our microgrid includes solar PV (generation), BESS

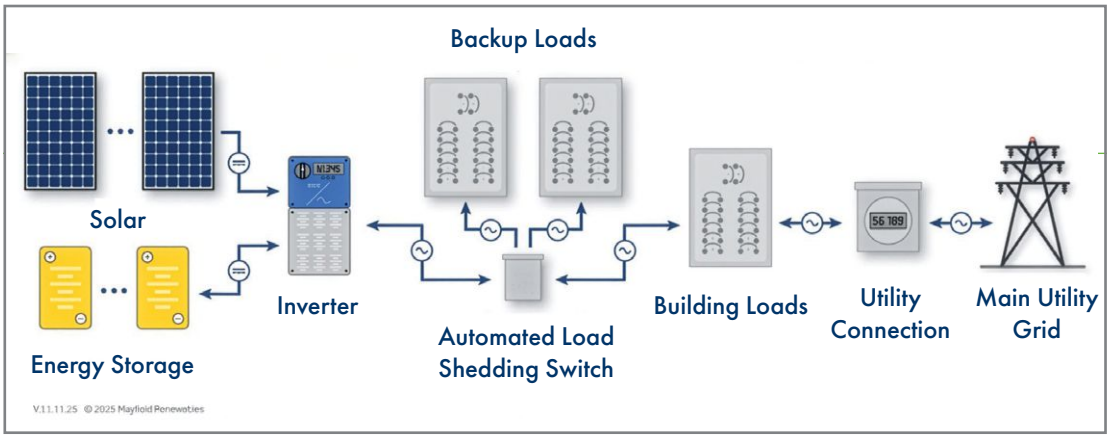


Figure 4: *Example Block Diagram*

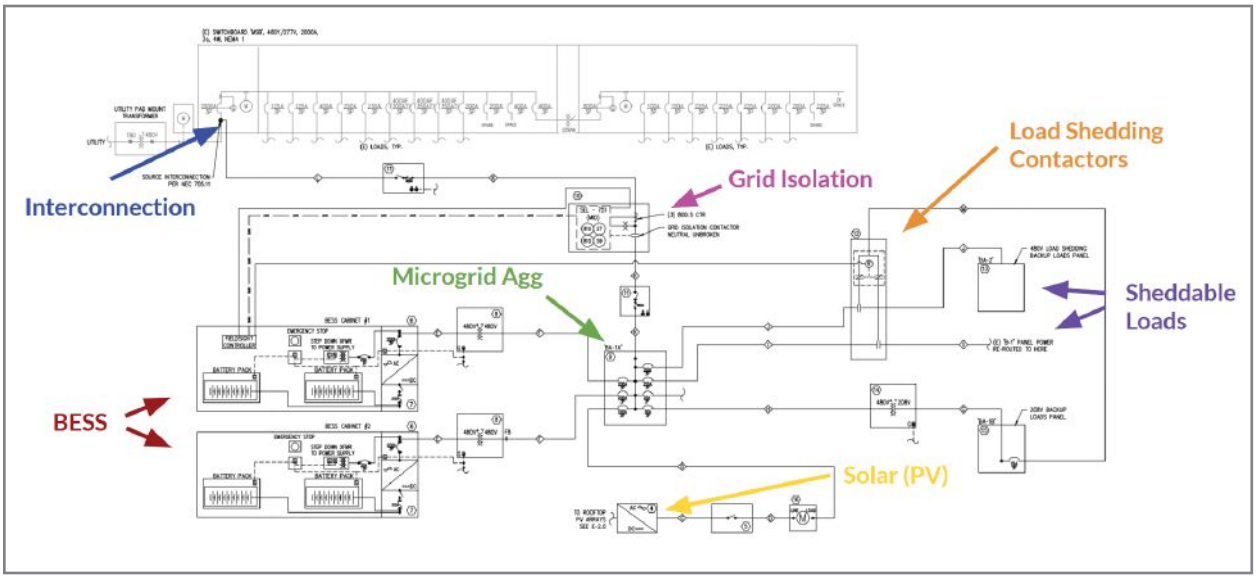


Figure 6: *Single-Line Diagram Showing Programmable Load Shedding*

(storage), a grid isolation device (islanding), and two groups of loads (primary backup and sheddable loads).

This microgrid system has two backup behaviors: full-facility and partial backup. During full-facility backup, non-sheddable loads (see Microgrid Agg panel in Figure 6), as well as the sheddable loads to the right side of the diagram, receive power. When the load-shedding threshold of the BESS SOC is reached, the load-shedding contactors, in communication with the controller integrated into the BESS, will transition from serving all loads to serving only the key loads located in the Microgrid Agg panel.

Lastly, as with many microgrid design considerations, note that the microgrid backup load management discussion can become more complicated and more dynamic. We described just one example above, but sophisticated market solutions can use real-time data to manage a load-shedding schedule algorithmically. In all cases, determining which loads will be backed up is a vitally important question to ask as early as possible in the microgrid design process.

DISPATCHABILITY OF ENERGY AND ENERGY STORAGE

The final important reminder is that energy storage is needed to fully leverage the benefits of any microgrid. It may not be obvious, but a system with only PV has little control over the exact timing of energy generation, as these kilowatts are intermittent in nature. Energy generation sources that are paired with storage become dispatchable and can fully optimize intermittent generation sources by storing otherwise curtailed PV energy. What's more, modern BESS products can stack multiple functions to accelerate a project's ROI and add more value to the broader grid. ■



TYSON BITTRICH *joined Mayfield Renewables, Inc. in 2023, and he is currently an Engineering Consultant, helping lead initiatives in education curriculum development and microgrid feasibility modeling. Bittrich is a member of the Sustainable Energy Action Committee's ESS Standards Working Group. He holds an MA in philosophy and a BS in renewable energy engineering from Oregon Tech.*

ENHANCING CYBERSECURITY IN THE ENERGY GRID: FROM MONITORING TO ENGINEERED RESILIENCE

BY KEON MCEWEN, *Black & Veatch*

The energy grid is becoming more connected, intelligent, and operationally dependent on digital systems every year. As utilities modernize infrastructure, integrate distributed assets, expand remote operations, and adopt data-driven tools, cybersecurity is no longer a support function on the sidelines of grid reliability; it's part of the reliability mission itself.



Today's grid requires a broader approach, one that combines visibility, disciplined governance, supply chain assurance, incident readiness, and security-by-design across the full infrastructure lifecycle.

In my work around operational technology (OT) cybersecurity, one thing has become clear: Cyber risk now sits at the intersection of physical operations, business priorities, and engineering decisions. It can no longer be treated as a narrow IT issue. It has to be addressed as part of how organizations design, operate, maintain, and recover critical infrastructure.

In practice, I still see organizations place perimeter defenses, compliance activities, and periodic assessments at the center of their cybersecurity programs. Those elements still matter, but they are no longer sufficient on their own. Today's grid requires a broader approach, one that combines visibility, disciplined governance, supply chain assurance, incident readiness, and security-by-design across the full infrastructure lifecycle.

In other words, the goal is no longer to be just secure enough to comply. The more practical goal is to be resilient enough to keep operating through disruption, make informed decisions under pressure, and recover quickly when incidents occur.

WHY THE GRID IS DIFFERENT

The electric grid differs from a traditional business operation in cybersecurity terms because cyber



PHOTO: © STOCK.ADOBE.COM/CONTRIBUTOR/212388843/RIFQI

incidents in OT environments can have direct physical effects. A compromised business system may interrupt administrative operations, but a compromised OT system can affect generation, transmission, power quality, protection schemes, or operational visibility where reliability matters most.

That distinction grows more important as legacy systems become increasingly connected, digitally monitored, and remotely operated. Smart sensing, automation, remote diagnostics, and analytical tools help operators improve performance and make better decisions faster. But every new interface, remote pathway, integrated service, and vendor dependency also expands the attack surface.

When I look at grid cybersecurity, I tend to frame it less as a technology problem and more as an operational and engineering problem with cybersecurity consequences. Improperly secured connections between IT and OT, internal and third parties, or field assets and centralized systems can create pathways that adversaries may exploit.

FROM POLICY TO OPERATIONAL GOVERNANCE

Policy remains essential because it establishes the baseline for how an organization intends to operate, what it values, and which controls it expects its people to follow. But in today's environment, policy alone is not enough.

Cybersecurity governance now has to keep pace with changes in remote access, third-party services, engineering design, and tools enabled by artificial intelligence (AI). That takes practical coordination across operations, engineering, cybersecurity, procurement, and vendor management.

The real test of governance is not whether a policy exists. It's whether the organization can make sound decisions consistently, especially when a project is

moving fast, a vendor needs access, or an operational issue needs to be solved quickly.

Once accountability is established, the next challenge is deciding how much trust should be granted to users, devices, vendors, and systems as they interact with operational environments.

ZERO TRUST, ADAPTED FOR OPERATIONS

As OT environments become more interconnected, Zero Trust cybersecurity principles are gaining attention across critical infrastructure. My view is that Zero Trust is useful in OT only when it's adapted to operational reality. It should not mean copying enterprise IT security models directly into plants, substations, control centers, or field networks. These environments have safety requirements, uptime constraints, and legacy technologies that demand a more careful and tailored approach.

Still, the core ideas of Zero Trust are increasingly relevant: stronger identity and access control, better asset visibility, secure communications, effective segmentation, and an assumption that trust should not be granted simply because a user or device is already inside the network boundary.

For utilities, this means building security in layers and reducing unnecessary implicit trust. Done carefully, that can limit lateral movement, improve accountability, and strengthen resilience without compromising operations.

Those same principles also shape how organizations evaluate internal visibility, because access decisions are only as strong as the asset, identity, and communication data behind them.



Zero Trust cybersecurity principles are gaining attention across critical infrastructure.

MONITORING IS EVOLVING INTO OBSERVABILITY

Monitoring remains one of the most important building blocks in industrial cybersecurity, but the conversation is shifting toward a broader concept: observability.

The question is no longer simply whether an organization collects logs or receives alarms. The more important question is whether it has enough visibility across assets, communications, identities, remote access paths, and process behavior to understand what normal looks like and identify meaningful deviations early.

This matters in OT because cyber incidents often don't look like cyber incidents at first. They may appear as a device malfunction, control instability, process upset, or unexplained operational disruption. Without adequate internal visibility, organizations may struggle to distinguish equipment failure from malicious activity until the impact becomes much larger.

That makes internal monitoring increasingly important. A lesson I keep coming back to is simple: If you cannot see it, you cannot confidently investigate it. Watching the perimeter isn't enough. Organizations also need insight into what's happening inside trusted environments so they can detect abnormal behavior, investigate events quickly, and support faster containment and recovery.

With governance setting accountability and observability and improving situational awareness, organizations are better positioned to evaluate advanced capabilities such as AI without treating them as a substitute for operational understanding.

AI IN OT: OPPORTUNITY AND RISK

AI has moved from an emerging concept to an operational consideration. Across the energy sector, AI-enabled capabilities are being explored for anomaly detection, predictive maintenance, operational decision support, and performance optimization.

These capabilities can offer meaningful advantages, but they also introduce new questions. How is the model trained? What data is it using? Who validates its output? What happens if it misclassifies

an event or behaves unexpectedly? And how much authority should an AI-enabled function have in an environment where safety and uptime are critical?

I don't think the answer is to avoid AI. The better answer is to be deliberate about where it fits, what it depends on, and how much authority it should have. In OT environments, I would treat AI like any other critical capability: Understand it, test it, monitor it, and integrate it with human oversight and fail-safe thinking. Used well, AI can improve visibility and decision-making. Used carelessly, it can introduce new risks into already complex environments.

The same disciplined approach should extend beyond internal tools to external providers, products, and services that increasingly support grid operations.

SUPPLY CHAIN RISK NOW A CORE CYBERSECURITY ISSUE

One of the biggest shifts in recent years is the growing recognition that supply chain risk is central to grid cybersecurity. Utilities depend on equipment manufacturers, software providers, system integrators, managed services, contract engineers, and remote support relationships. That means the attack surface extends far beyond the organization itself.

Cybersecurity must therefore include a closer look at vendor remote access, software integrity, patch provenance, contractual security requirements, and the processes used to introduce updates or changes into the environment.

This is also where management of change becomes stronger cyber control. In practical terms, third-party laptops, removable media, temporary engineering access, service updates, and support connections all need to be tracked, authorized, and evaluated in the context of cyber risk, not just operational convenience.

Effective change management creates traceability, provides early warning signs, and helps organizations prevent avoidable exposure before a small issue becomes a major incident. Even with strong governance, visibility, access control, AI oversight, and supply chain discipline, utilities must still plan for the possibility that disruption will occur.

RESILIENCE MEANS RECOVERY, NOT JUST PROTECTION

Resilience remains as important as ever, but organizations are becoming more precise about what it should mean in practice. It includes preparedness, detection, containment, response, recovery, and follow-through. It also requires meaningful ways to measure progress.

Organizations often focus heavily on prevention, but the most mature programs also invest in how they will operate during disruption and how quickly they can restore stability afterward. In real-world response planning, success is not measured only by whether every threat was blocked. It's also measured by how effectively the organization can continue operations, recover trust in the system, and reduce the time and cost of disruption.

Incident response in OT must also remain a cross-functional discipline. Operators, engineers, network personnel, cybersecurity staff, and external experts all have a role because OT events often require technical interpretation before they can be correctly classified. Distinguishing between equipment failure, process upset, misconfiguration, and malicious activity takes both visibility and experience.

The most durable resilience strategy is the one that reduces preventable weaknesses before systems are installed, commissioned, or connected to operational environments.



THE STRONGEST DEFENSE STARTS IN DESIGN

One of the most important shifts in the industry is the recognition that the best time to address cyber risk is before assets are deployed. Secure-by-design and cyber-informed engineering (CIE) approaches push cybersecurity upstream into architecture, design, procurement, and implementation rather than leaving it as a later retrofit exercise.

For energy projects, that means asking cybersecurity questions early. Do the switches and communication paths support the necessary security capabilities? Is remote access necessary, and if so, how will it be controlled? Does the architecture provide the right segmentation? What visibility will operators have once the environment is live? How will vendors connect? How will changes be governed over time?

These are engineering questions as much as cybersecurity questions. In my experience, answering them early is one of the most reliable ways to reduce long-term risk, avoid costly retrofit work, and improve resilience before the system ever becomes operational.

RESILIENCE: THE REAL DESTINATION

The energy grid's cybersecurity challenge is no longer simply about protecting connected assets from external attacks. It is about building systems that can withstand modern threat conditions while continuing to support reliable operations in a highly connected, fast-changing environment.

The strongest programs treat cybersecurity as part of the lifecycle, not something added after design, procurement, or commissioning decisions have already been made.

Compliance remains important, but compliance is not the destination. The real objective is resilience: the ability to detect earlier, respond faster, recover with confidence, and design infrastructure that is harder to disrupt in the first place.

As the grid becomes more digital and intelligent, cybersecurity must be more than a control function. It must become a design principle for the future of energy infrastructure. ■



The strongest programs treat cybersecurity as part of the lifecycle, not something added after design, procurement, or commissioning decisions have already been made.



KEON MCEWEN, *Head of Solutions Development and Industrial Cybersecurity at Black & Veatch, has a history in cybersecurity. He started his career as an electrical engineer in control systems and process control engineering. From there, he was drawn into cybersecurity, where he used his knowledge of operations technology (OT) and industrial control systems (ICS) to help protect power systems. McEwen joined Black & Veatch, which has offered cybersecurity services for more than 15 years, to help expand their industrial cybersecurity services by establishing a dedicated department focused on building solid consistency across projects.*

NETA ANNOUNCES AN **EPIC** EVENT!

EPIC Electrical Power Innovations Conference

An InterNational Electrical Testing Association Event

See the complete Schedule At A Glance in the **Fall 2026** issue of ***NETA World*** **Journal!**

REGISTER NOW AT:
EPICpower.org

Join industry experts, innovators, and leaders at the premier educational conference focused on the future of electrical power.

Join your colleagues!

- *Grid Optimization & Smart Grid Management*
- *Renewable Integration & Energy Storage Innovation*
- *AI Potential To Revolutionize The Energy Management Sector*
- *Cybersecurity-Enabled Power System Operations*
- *Policy, Regulation, and Standards Shaping System Design*
- *Fueling The Next Generation Of Talent*

REGISTER TODAY

October 11–13, 2026

Sheraton Fort Worth | Fort Worth, TX

Visit EPICpower.org today for more information

DIGITAL SUBSTATION APPLICATION CONCEPTS FOR IBR RENEWABLE ENERGY PLANTS

BY WAYNE HARTMANN, *GE Vernova, USA*

With the fast-tracked planned installations of utility-scale inverter-based resource (IBR) power plants to the bulk power system, utilities, consultants, EPC contractors, and developers are all seeking methods to standardize protection and control (P&C) designs to hasten project execution. Many of these power plant designs incorporate a high-voltage (HV) section or sections, a pooling bus (PLB) section or sections, and collector bus (CLB) sections.

This article explores a typical utility-scale photovoltaic IBR power plant incorporating all these sections and suggests architectures for standardized yard-to-merging unit connectivity. It also addresses the use of partially centralized protection solutions to hasten project execution and further increase standardization. As most of these power plants follow standardized approaches for the power infrastructure, the protection and control can also provide a high degree of standardization.

RENEWABLE POWER PLANT DESIGN

CLBs and PLBs are used in renewable power plants such as wind or photovoltaic (PV) power stations to manage the power flow from the generation source to the transmission grid. In these distributed generation projects, power is produced by many individual sources, such as wind turbines or solar panels. Each of these sources generates a relatively small amount of power at low- or lower medium-voltage levels (480 V–4.160 V).

The collector substation aggregates this power and combines it into a major block of power at a higher medium voltage (13.8 kV–69 kV). These major blocks of power are then combined into output that can be fed into the transmission grid at HV level (115 kV–230 kV plus). Managing and utilizing the power generated by these distributed sources would be difficult without CLBs and PLBs, which serve as critical links between the renewable power sources and the main power grid.

Factors to consider in CLB and PLB designs:

- The design seeks to minimize losses and voltage drops within budgetary constraints.
- Factors considered in interconnecting cable design include cost, real power losses, and voltage drop. A typical design goal is to keep average real power losses below 1%. At full output, real power losses can be as much as 2% to 4%.
- Interconnecting cabling from IBR sources to the collector buses and to step-up transformers between the collector and pooling buses is typically underground.
- Metal-clad switchgear in weatherproof enclosures is often used for CLBs at 15 kV and below.
- At higher medium-voltage levels, PLBs are typically outdoor air-insulated designs using vacuum breakers.

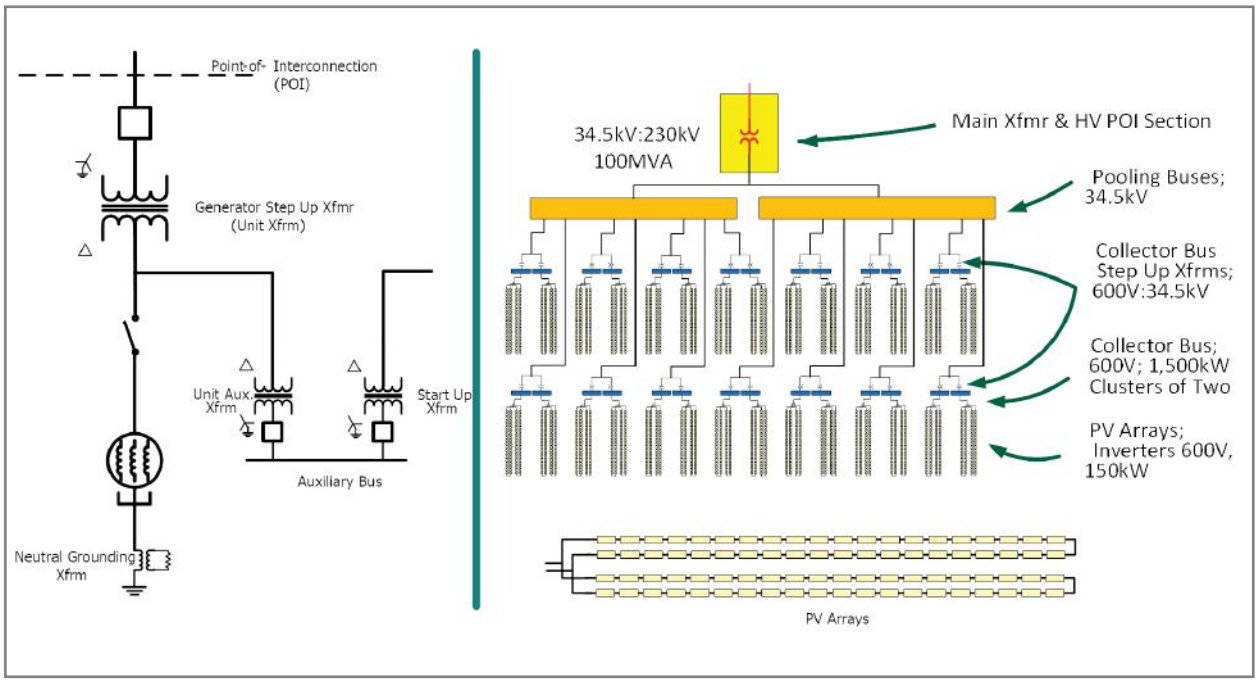


Figure 1: *Comparison of Traditional and IBR Renewable Power Plants*

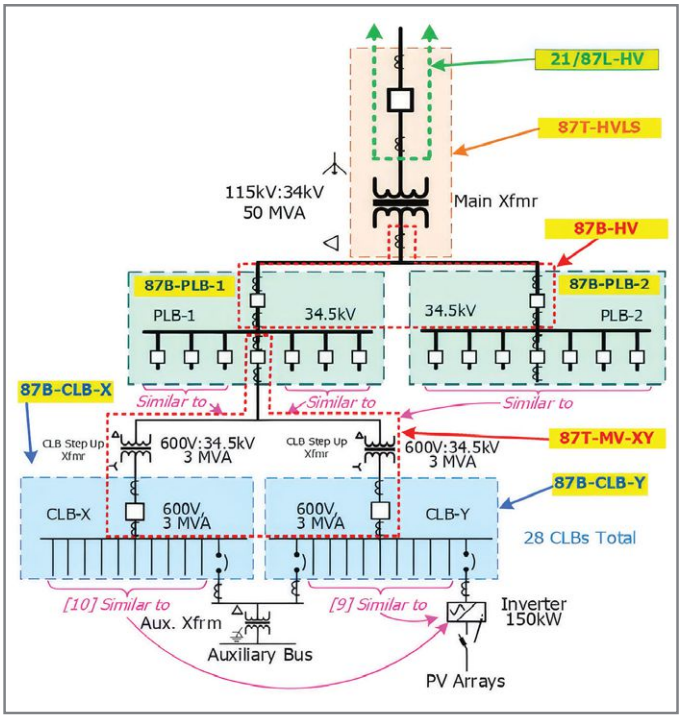


Figure 2: *Utility-Scale Solar Plant*

Figure 1 compares and contrasts a traditional utility-scale powerplant with a single power source with an IBR renewable plant with hundreds of smaller energy sources.

The plant's various buses and voltage levels are listed below:

- Two identical PLBs are used, each with seven sources: air-insulated switchgear (AIS) and outdoor CBs.
- Seven identical sources feed each PLB input.
- The 28 CLBs are identical LV switchboards in weather-proof enclosures.
- CLB connections are 10 150-kW, 600-V inverters, a feeder to supply auxiliary power, and one output to the CLB step-up Xfmr.
- Two CLBs are grouped per PLB input.
- Two PLBs are input into the main Xfmr.

We will make use of standard infrastructure topology to develop a standard approach to the protection schemes using digital substation techniques.

PROTECTION PHILOSOPHY AND DESIGN

An economic protection method is to employ partially centralized systems with the collector

and pooling buses. Partially centralized systems combine an element suited for a given zone or zones of protection, plus multizonality, which protects different zones with the same protection system.

For our study, we assume two protection systems are used for application in partially centralized distribution protection schemes:

- **System #1.** A transformer protection system that can cover <=6 nodes, using a definable and selectable transformer differential zone, with all nodes employing overcurrent, voltage, and frequency elements.
- **System #2.** A combination bus/feeder, main, tie CB protection system that can cover <=28 nodes of primary bus differential protection with phase and neutral/ground overcurrent, overvoltage, neutral overvoltage and breaker failure protections for each node. The differential protection can be divided into <=3 zones.

Single-line drawings (SLD) of the two systems are shown in Figures 3, 4, 5, and 6.

Figure 2 describes the infrastructure and protection application:

- For CLB main CBs and the cabling to the main Xfmr low-side CTs, one System #2 will cover two CLB main CBs and cabling to the main step-up Xfmr low-side winding.
- For the main Xfmr, two System #1s will provide redundant coverage.
- For the HV utility POI, two-line protection systems will provide coverage.
- Six modular units (MUs) will be used to provide redundant HV POI line protection, redundant main Xfmr protection, and non-redundant PLB to main Xfmr low-side bus protection.

This will be shown in detail from the CLB to the utility point of interconnection (POI).

SYSTEM #1

Figure 3: *Multifunction, Multizonal (Centralized) Transformer Differential and Feeder/ Main/Tie Protection System SLD*

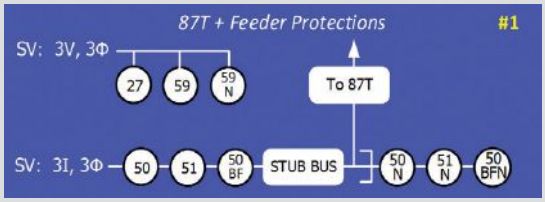
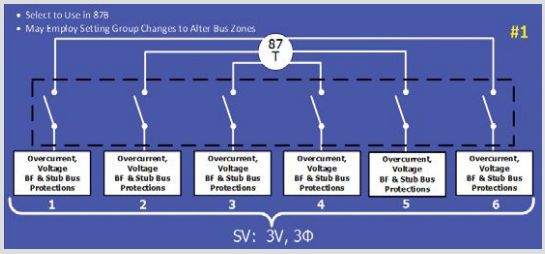


Figure 4: *87T Selectivity for Multifunction, Multizonal (Centralized) Bus Differential and Feeder/ Main/Tie Protection System*



SYSTEM #2

Figure 5: *Multifunction, Multizonal (Centralized) Transformer Differential and Feeder/ Main/Tie Protection System SLD*

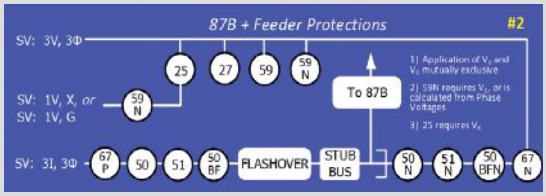
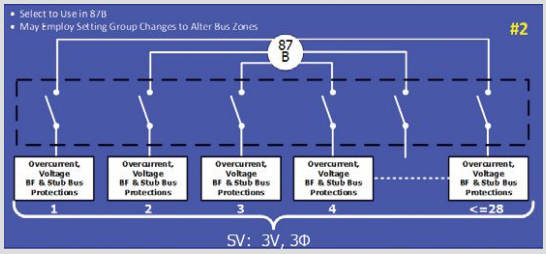


Figure 6: *87T Selectivity for Multifunction, Multizonal (Centralized) Bus Differential & Feeder/ Main/Tie Protection System*



Figures 3, 4, 5, and 6: *Bus Differential and Feeder/Main/Tie Protection System*

MU Connectivity and Protection: CLB

Figure 7 describes the infrastructure and protection application for CLBs; System #2 will cover two CLBs.

- Seven groups of two CLBs per PLB input; two CLBs are connected to each PLB.
- Each CLB has 10 inverters, one auxiliary source, and one main as nodes (12 nodes total).
- Overcurrent, voltage, and breaker failure protection are provided for all nodes.
- Each CLB is a 12-node 87B zone, 87CLB-X, and 87CLB-Y.
- Total nodes used by CP#2 = 12+12 = 24 (<=28).
- Non-redundant protection for the set of two CLBs will require one Protection System #2.
- Non-redundant protection for the set of two collector buses application will require 14 MUs.
- For nodes on the CLB, System #2 provides bus differential protection. For a bus differential trip, all CBs connecting the CLB are tripped.
- A breaker failure (BF) of the main CB will be cleared by an upline PLB input CB.

Note: *All MU-relay signals are transmitted through a networked connection. Connections shown here show relationships only.*

MU Connectivity and Protection: CLB to PLB, CLB 87B

System #1 provides overcurrent, voltage, and BF protections for the two CLB main CBs and the PLB input CB (Figure 8). The respective CB is tripped for any protection trip. In the case of BF, all CBs connecting the CLB are tripped.

System #1 provides transformer and cable differential protection for the zone between the two CLB CBs and the PLB input CB. For a transformer or cable differential trip, two CLB CBs and a PLB input CB tripped. A BF of a PLB input CB will clear the respective PLB.

MU Connectivity and Protection: PLB

System #2 provides overcurrent, voltage, and BF protections for the PLB input and main CBs (Figure 9). The respective CB is tripped for any protection trip. In the case of BF, all CBs connecting the PLB are tripped.

System #2 provides bus differential protection for nodes on the CLB. For a bus differential trip, all CBs connecting the CLB and PLB tripped. A BF of a PLB main CB will trip CB M.

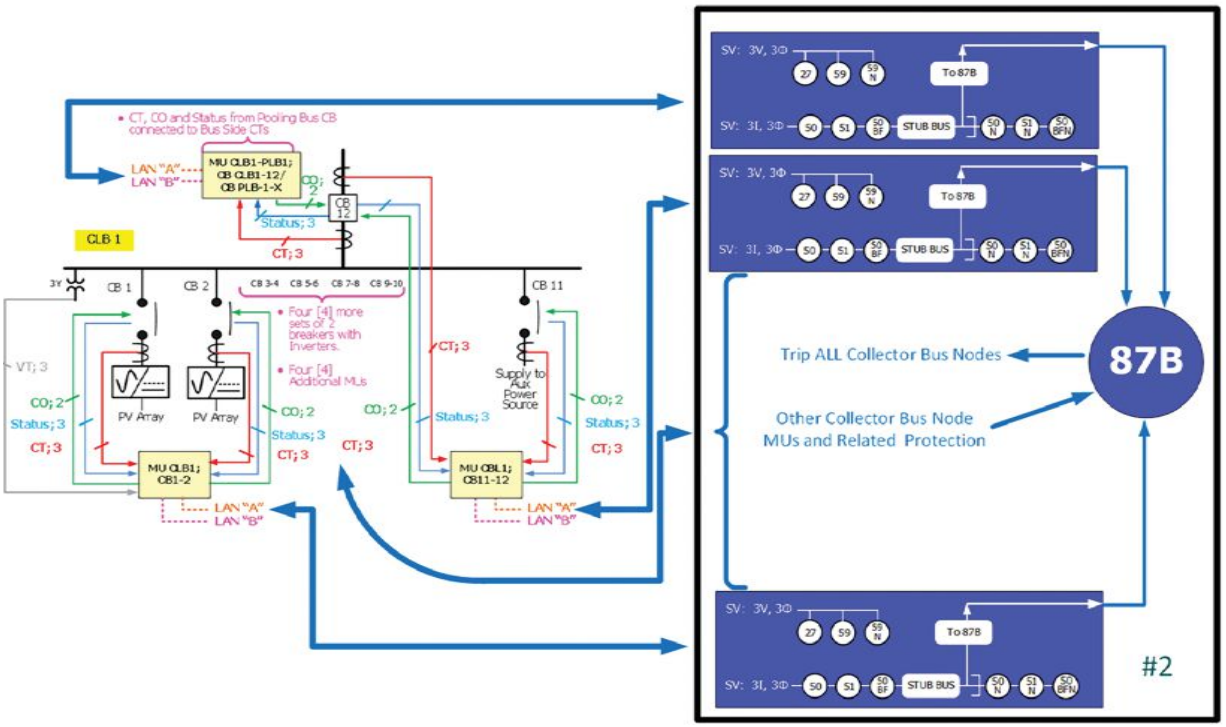


Figure 7: *MU Connectivity and Protection: CLB*

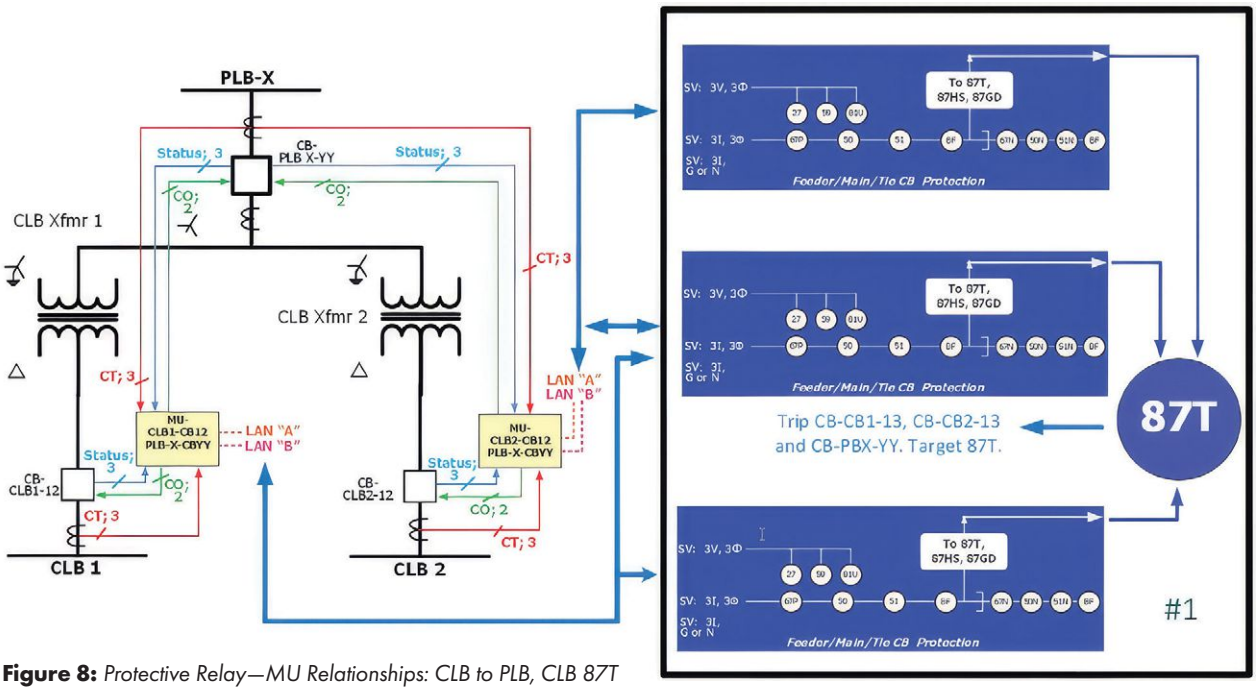


Figure 8: *Protective Relay—MU Relationships: CLB to PLB, CLB 87T*

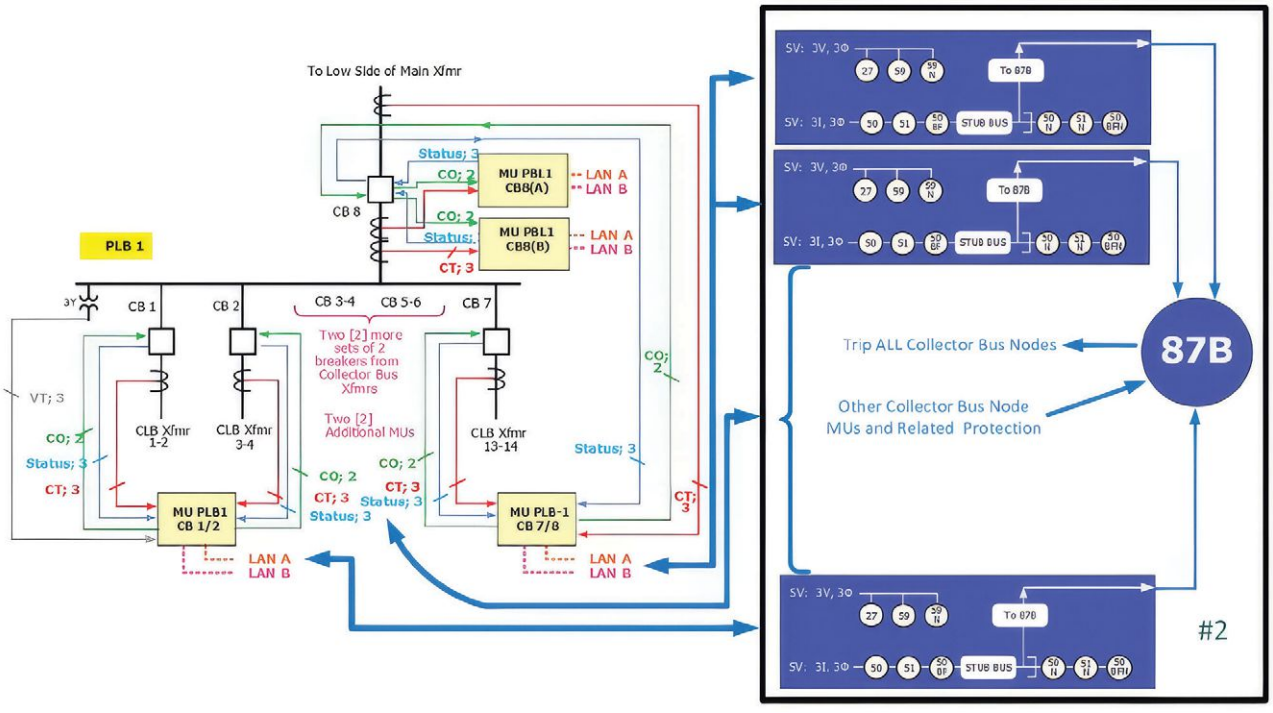


Figure 9: *Protective Relay—MU Relationship: PLB*

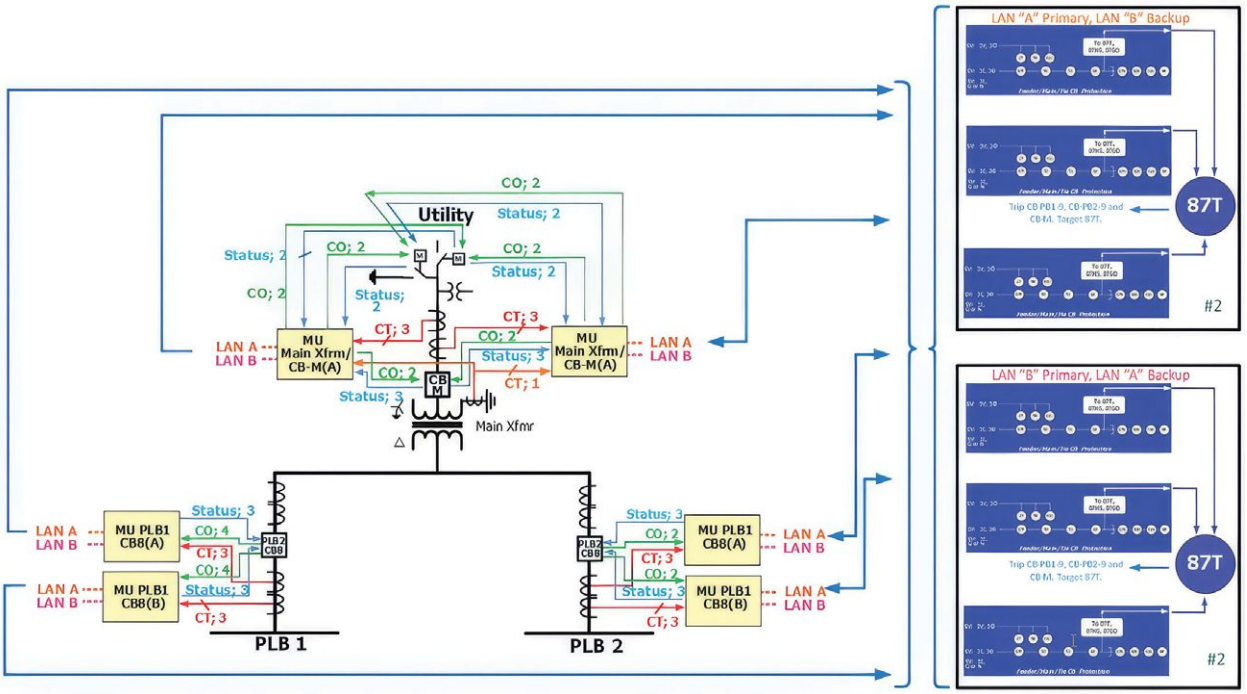


Figure 10: *Protective Relay—MU Relationships: Main Xfmr 87T*

Description of infrastructure and protection application:

- System #2 will cover two CLBs.
- Yard-to-MU connectivity for PLB 1; PLB 2 is similar.
- Non-redundant protection for the set of two CLBs will require one Protection System #2.
- Total nodes used by CP#2 = 8+8 = 16 (<=28).
- Non-redundant protection for the set of two collector bus applications will require eight MUs.
- Redundant MUs on the PLB Main CB bus side are part of the main Xfmr 87T (HV, NERC).

Protective Relay – MU Relationships: Main Xfmr 87T

System #2 provides overcurrent, voltage, and BF protections for the two PLB Main CBs (Figure 10). The respective CB is tripped for any protection trip. In the case of BF, all CBs connecting the PLB are tripped.

System #2 provides bus differential protection for the two PLB Main CBs, cables between the PLB and Main Xfmr, the Main Xfmr, and CB-M. For a bus differential trip, all CBs connecting the PLB and the utility POI (main CB) are tripped. Two System #2s are used for the required redundancy. A BF of a PLB output CB will clear all respective PLB CBs. A BF of CB-M will transfer the trip to the upline transmission system CBs.

MU Connectivity and Protection: Utility POI

The utility POI dual-line protection systems are employed for the CB-M (Figure 11). Exact element fleet and principle used are dependent on the bulk system owner. CB-M is tripped for any line protection that trips in either redundant protection system. A BF of CB-M will transfer the trip to the up-line transmission system CBs.

CONCLUSION

- In some utility-scale IBR renewable plants, a high quantity of granulized and repeated power infrastructure may be used. These designs lend themselves to the use of centralization for a high degree of standardization in the P&C design.
- Savings on the number of protective devices, panels, and space inside the control house can be obtained. In Greenfield applications, MUs

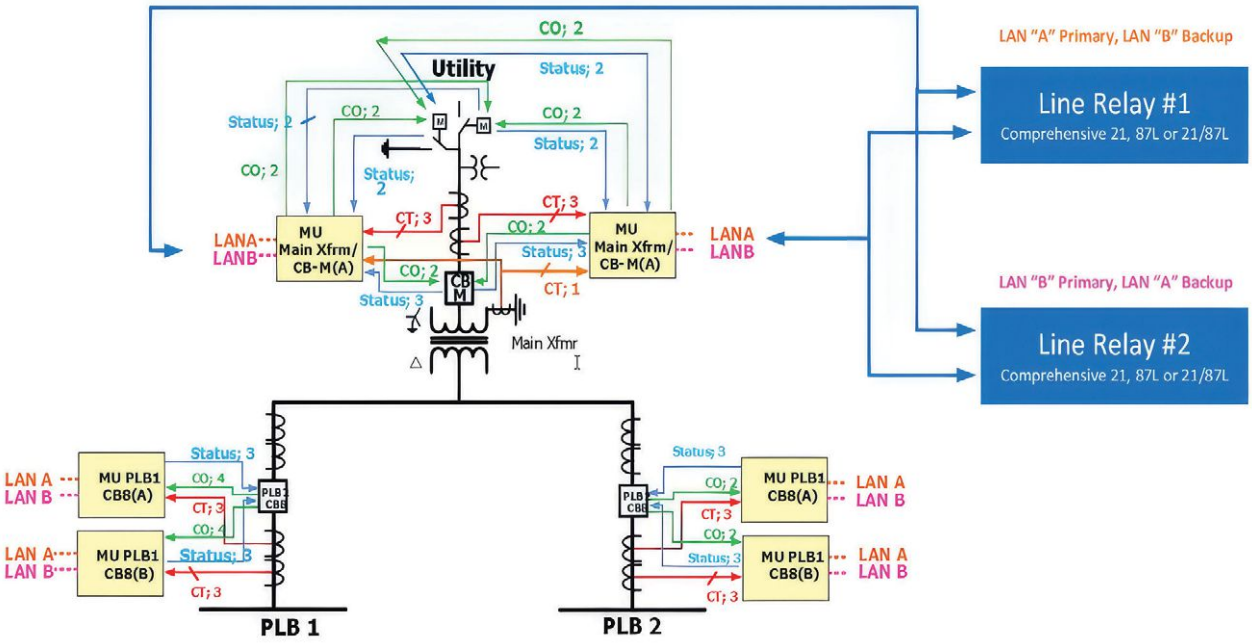


Figure 11: *Protective Relay—MU Relationships: Utility POI*

can often be housed in breaker cabinets and LV switchgear compartments, with attendant enclosure and civil savings.

- As one of its attributes, centralization allows economical application of primary and backup functions, and a significant amount of standardization can occur from the standardized design and fabrication of MU enclosures (if applied). Wiring runs from MUs to the yard elements are short and standardized.
- It is possible to protect high-node-count buses using process bus-enabled protection.
- It is possible to economically deploy cable differential protection using sampled values from cable terminals and defining the cable as a bus zone.
- If the MU information for all accessed points is brought into the control house, operators have full view of every element of the plant, from the high-voltage POI to the individual inverter AC inputs, without having to travel to various areas of the plant. ■



WAYNE HARTMANN *is an Advanced Applications Advisor for GE VERNOVA, Grid Automation. He explores the application of new technologies in protection and control with electric utilities, industrials, and consultants. He provides market research and ideation for new product development and supports the sales and application teams. Hartmann was in Standards Development at Duke Energy and in Application, Sales and Marketing Management capacities at Beckwith Electric, PowerSecure, GE, Siemens Power T&D, and Alstom T&D. He is a Life Senior Member of IEEE and has served as a main PSRC Committee member for over 30 years, contributing to standards, guides, reports, and tutorials.*



PROVEN BEFORE THEY EVEN REACH THE FLOOR.

Our technicians train on industry equipment, in conditions that mirror yours, through programs designed with industry. **The result?**

People ready to contribute from **day one** – so your growth isn't capped by who you hire.

TRAIN
YOUR TEAM.

HIRE
A TECHNICIAN.

GROW
WITH US.

TSTC
Texas State Technical College

tstc.edu

Vacuum Interrupters
A Group CBS Company

POWERED BY M18 REDLITHIUM

LRTS10
CONTACT RESISTANCE TEST SET

MEET THE LRTS10

The industry's first Milwaukee® battery-powered micro-ohm meter

INTERCHANGEABLE. UNSTOPPABLE.
Works with all Milwaukee® M18™ batteries, giving you the flexibility to swap batteries and keep working.

10A TEST CURRENT RANGE UP TO 10 AMP
LRTS10 has a test current range up to 10 amp.

WHY THE LRTS10?

MILWAUKEE® BATTERY POWERED
Cordless freedom with the power and reliability you expect from Milwaukee

RESULT LOCK OPTION
Lock in your readings for confidence in every measurement

TEST STATUS INDICATORS
Audible and visual indicators keep you informed at every step of the test

USER FRIENDLY & SIMPLE
Easy to learn and simple to use

FREEDOM THAT DOESN'T RUN OUT.

Battery-powered testing isn't new.
A truly interchangeable battery system is.

The **LRTS10** is the first battery-powered micro-ohm meter to utilize the trusted Milwaukee® M18™ battery platform, allowing you to swap batteries in seconds and keep testing without waiting for an internal battery to recharge.

Already invested in Milwaukee tools? Simply use the same batteries you already own. Need more runtime? Carry a spare battery and keep working.





INCLUDES BATTERY AND CHARGER
Includes one Milwaukee® M18™ battery and charger. Everything you need to power up, charge up, and get the job done.

INTERCHANGEABLE BATTERY SYSTEM
Compatible with all Milwaukee® M18™ batteries. Swap batteries. Keep working.

LIGHTWEIGHT & PORTABLE
Built for the field.
Easy to carry, easy to use.

BUILT TO PERFORM
Rugged construction designed to withstand tough environments.

vacuuminterrupters.com
Sales · Service · Support

The POWER of ONE™ GROUP CBS