© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1719675

# Busbar Protection Schemes: Centralized Vs Distributed, And Dependability/Security Assessment

HUMAYUN RAFIS

***Abstract-*** ***Busbar protection is among the most critical functions in substation protection because a bus fault can interrupt multiple circuits at once, damage primary equipment, and rapidly escalate into a wide-area outage. At the same time, substation digitalization has changed the engineering basis of busbar protection. Modern schemes may be hardwired, IEC 61850-enabled, process-bus-based, centralized, distributed, or virtualized, and each architectural choice reshapes not only speed and selectivity but also maintainability, interoperability, and cyber exposure. This review compares centralized and distributed busbar protection schemes and develops a structured framework for dependability and security assessment. The study follows a protocol-driven review methodology focused on literature published between 2020 and 2025, with attention to bus differential protection, process bus design, synchronization, redundancy, interoperability, virtual IEDs, testing, and cybersecurity. The paper finds that centralized architectures provide a coherent system-wide view and simplify some forms of protection coordination, but they concentrate timing, software, and cyber risks. Distributed architectures improve modularity, support phased retrofit, and often degrade more gracefully under isolated failures, but they increase configuration-management burden and interoperability demands. The review argues that architecture alone does not determine performance. Dependability and security emerge from the interaction of differential algorithms, current-transformer behavior, topology processing, network redundancy, sampled-value quality, time synchronization, cyber controls, and maintenance practice. For most utilities, the most resilient pathway is not purely centralized or purely distributed but hybrid: distributed acquisition, deterministic communication, redundant timing and networking, disciplined configuration governance, and hardware-in-the-loop validation supported by IEC 62351-aligned cyber protections. The paper concludes by identifying research gaps and by proposing a practical assessment framework for procurement, FAT/SAT, commissioning, and lifecycle review.***

***Keywords: Busbar Protection, Differential Protection, Centralized Protection, Distributed Protection, IEC 61850, Digital Substation, Process Bus, Dependability, Security, Cybersecurity***

## I. INTRODUCTION

A busbar is electrically compact but operationally decisive. It is the node that concentrates incoming and outgoing circuits, interconnects feeders, transformers, and tie lines, and determines how quickly energy can be rerouted or interrupted during a disturbance. That makes busbar faults rare but disproportionately severe.

When a fault occurs inside the protected bus zone, the protection system must isolate the fault almost instantaneously while preventing unnecessary disconnection of healthy circuits. In practice, that means busbar protection must satisfy four demanding requirements at once: speed, selectivity, dependability, and security (Lima et al., 2022; Song et al., 2020; Vásquez & Silva, 2021).

The historical answer to that challenge has been differential protection backed by carefully engineered CT circuits, topology-selection logic, and breaker-failure interaction. Yet the conditions under which differential protection is implemented have changed.

Digital substations move signaling away from point-to-point copper and toward IEC 61850 process bus and station bus communications. Merging units, sampled values, GOOSE messaging, software-defined logic, virtual IEDs, and multivendor engineering tools are now part of the protection environment.

This transition opens major opportunities - reduced wiring, flexible engineering, richer monitoring, faster retrofit, and easier system integration - but it also moves critical protection dependencies into the communication, synchronization, and cyber layers (Bhattacharjee et al., 2022; Diaz et al., 2020; Gaspar et al., 2023).

A consequence is that architecture matters more than ever. In a centralized busbar protection scheme, protection intelligence is concentrated in a central processor or platform that receives information from the bays, decides zone membership, evaluates differential quantities, and issues trips.

In a distributed scheme, those functions are partitioned among bay-level or near-bay devices and coordinated through deterministic communications. The two architectures can protect the same primary layout, yet they create different failure modes, maintenance burdens, and cyber exposures.

Therefore, comparing their protection algorithms alone is insufficient. What is needed is an integrated assessment of how architecture affects protection dependability, operational security, and cybersecurity.

This paper responds to that need. It reviews recent literature on busbar protection, digital substation architectures, reliability and availability analysis, process bus implementation, synchronization, interoperability, virtualized protection, and cyber resilience.

It uses that literature to compare centralized and distributed schemes and to propose a practical dependability/security assessment framework that utilities can apply during planning, procurement, testing, commissioning, and periodic review.

The section progression intentionally follows the formal structure of the uploaded sample paper - background, review, methodology, discussion, conclusions - while redesigning the methodology for a review article rather than a survey-and-simulation case study.

## II. UNIQUE REVIEW OBJECTIVES AND RESEARCH QUESTIONS

This review was designed to contribute something more specific than a general overview of digital substations. Five distinctive objectives guided the paper.

| Objective | Contribution |
|---|---|
| O1 | Separate architecture-level differences between centralized and distributed busbar protection instead of treating digital protection as a single category. |
| O2 | Compare schemes through explicit dependability and security criteria, including synchronization error, packet loss, CT saturation, common-cause failure, and cyber compromise. |
| O3 | Link relay behavior to communication architecture, redundancy, interoperability, diagnostics, and maintenance practice. |
| O4 | Identify which operating contexts favor centralized, distributed, or hybrid designs across greenfield and retrofit substations. |
| O5 | Propose a practical assessment framework for specification, FAT/SAT, commissioning, and lifecycle governance. |

RQ1: How do centralized and distributed busbar protection schemes differ in information flow, tripping logic, and architectural vulnerability?

RQ2: Which architecture is more dependable under realistic disturbances such as CT saturation, sampled-value distortion, synchronization error, or component failure?

RQ3: Which architecture is more secure against unwanted operation caused by design defects, maintenance mistakes, or cyber manipulation?

RQ4: Under what conditions is a hybrid digital architecture more attractive than a purely centralized or purely distributed one?

## III. REVIEW METHODOLOGY

Because this is a review paper, the methodology emphasizes transparent source selection, thematic coding, and comparative synthesis rather than primary field data. The procedure mirrors the method-first discipline of the uploaded sample paper but adapts it to literature review.

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1719675

Sources published from 2020 to 2025 were prioritized in order to capture present-day digital-substation practice. Search terms combined “busbar protection”, “bus differential protection”, “IEC 61850”, “centralized protection”, “distributed protection”, “process bus”, “GOOSE”, “sampled values”, “digital substation”, “dependability”, “security”, “cybersecurity”, “time synchronization”, and “interoperability” in various Boolean combinations (Lima et al., 2022; Muhammad & Saha, 2024; Silveira et al., 2023).

Inclusion criteria required direct relevance to at least one of the following themes: busbar differential protection, centralized or distributed digital substation architecture, process bus implementation, reliability and availability analysis, time synchronization, interoperability, virtualized protection, cybersecurity of relay or substation communication systems, or practical testing and commissioning.

Excluded were sources that discussed power-system protection in only a generic sense, papers that were unrelated to substation protection architecture, and studies whose main contribution could not be connected to the centralized-versus-distributed comparison.

After screening, each source was coded against seven analytical dimensions: architecture, measurement chain, communications and synchronization, internal-fault dependability, restraint security against external or distorted conditions, resilience to component or network failure, and lifecycle implications such as testing, interoperability, and maintainability.

This procedure allowed the review to move from description to structured comparison. It also aligns with recent work proposing structured impact-assessment models for digital substations and IEC 61850-based communication architectures (Santos & Zancul, 2023; Ayello & Lopes, 2023; Mathebula & Saha, 2022).

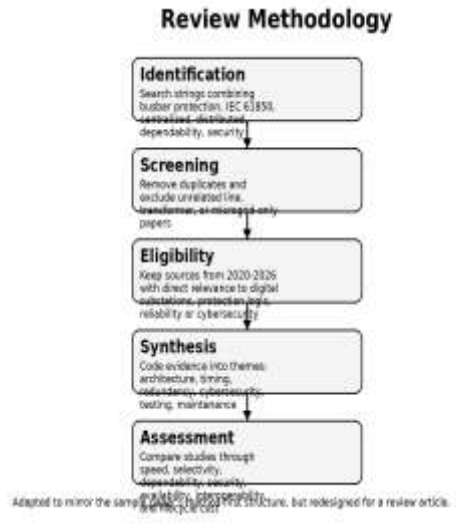


Figure 1. Review methodology used in this paper.

| Included evidence | Excluded evidence |
|---|---|
| 2020-2025 sources directly related to busbar protection or digital substation protection architectures | Pre-2020 papers used as primary evidence |
| Journal articles, conference papers, surveys, standards, and technical reports with explicit engineering value | General smart-grid papers without busbar or substation-protection relevance |
| Studies allowing dependability or security interpretation | Sources lacking enough technical detail for comparison |
| Work on process bus, synchronization, interoperability, redundancy, and cyber protection where these affect busbar protection performance | Unrelated protection functions unless they informed the architecture discussion |

## IV. TECHNICAL FOUNDATIONS OF BUSBAR PROTECTION

The dominant busbar protection principle remains differential protection. Currents entering and leaving the protected zone are compared, and the relay trips when the operating quantity exceeds a restrained threshold consistent with an internal fault. Modern low-impedance implementations use percentage

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1719675

restraint, topology processing, CT supervision, and dynamic bus replica logic.

Contemporary research does not reject this principle; it refines it through alternative signal-processing or pattern-recognition approaches such as generalized alpha-plane methods, superimposed current comparison, Lissajous-curve analysis, and machine-learning-based fault diagnosis (Vásquez & Silva, 2021; Joband et al., 2023; Sarlak, 2024; Jiang et al., 2024).

The first classical difficulty is discrimination between internal and external faults under transient distortion. External faults can produce severe CT saturation and create spill current in the differential quantity. If the scheme is too sensitive, security suffers. If it is too restrained, dependability or speed suffers.

This balance has always been central to busbar protection, but digital substations add new distortions that are not purely electromagnetic. Data desynchronization, sampled-value loss, VLAN or multicast misconfiguration, virtual-circuit errors, and engineering-file mistakes can all imitate or mask differential behavior (Song et al., 2020; Cao et al., 2024; Liu et al., 2025).

A second foundation is topology awareness. Busbar protection must know which primary elements presently belong to the protected zone. In conventional systems this is often achieved by hardwired auxiliary contacts and fixed bay logic. In digital substations the same function may be achieved through GOOSE subscriptions, software bus replica models, or centralized configuration repositories.

That increases flexibility, especially in substations with sectionalizers and transfer buses, but it also makes protection quality depend on configuration integrity and interoperability. A tripping algorithm is only as good as the topology information that reaches it (Ayello & Lopes, 2023; Bhattacharjee et al., 2022; Chen et al., 2021).

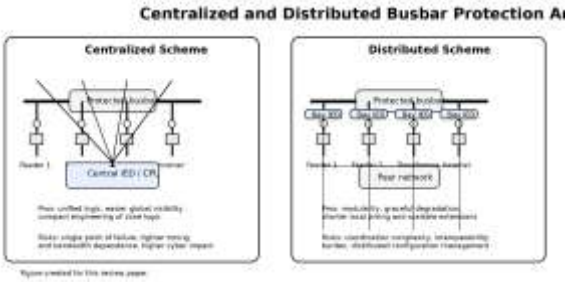


Figure 2. Conceptual comparison of centralized and distributed busbar protection architectures.

## V. CENTRALIZED BUSBAR PROTECTION SCHEMES

In a centralized scheme, currents or preprocessed measurements from multiple bays are delivered to a central protection processor that performs topology determination, differential computation, supervision, and tripping. The architecture may still employ bay devices for acquisition or interface functions, but protection intelligence is concentrated in one logical location.

In digital substations that central point may be a dedicated central IED, a centralized PAC platform, or, increasingly, a virtualized application executed on resilient computing hardware (Song et al., 2020; Kabbara et al., 2022; Rösch et al., 2024).

The main technical attraction of centralization is unified system visibility. A central processor can observe all bay currents, all topology states, and all zone relationships simultaneously. This can simplify bus replica logic, breaker-failure interaction, event analytics, and coordinated protection functions that would otherwise need peer-to-peer exchanges.

Centralized logic also aligns with wider protection, automation, and control trends that seek to consolidate decision making and reduce duplicated functionality across bay devices (Rubio et al., 2025).
From a dependability perspective, centralized schemes can perform extremely well when data quality is coherent. Song et al. (2020) showed that centralized busbar differential protection in an IEC 61850 environment can operate securely and accurately if data desynchronization is explicitly compensated.

Their work is important because it exposes the defining vulnerability of centralized digital protection: the processor does not merely need correct values; it needs correct values that are temporally coherent. Measurement timing error and synchronization error become protection errors, not just communication imperfections.

A further strength of centralized architecture is analytic richness. Centralized platforms can host advanced diagnostics, self-supervision, disturbance recording, cybersecurity monitoring, and adaptive logic more naturally than fragmented architectures.

This becomes even more relevant as virtualized protection and software-defined substation platforms mature. However, the same concentration that simplifies analytics magnifies common-mode risk. If the central processor, hypervisor, time source, or software image fails, the whole protection zone can be compromised. Thus, centralization improves observability but enlarges blast radius (Kabbara et al., 2022; Rösch et al., 2024; Rubio et al., 2025).

For that reason, centralized busbar protection is most credible when supported by disciplined communications engineering, redundant timing, deterministic network behavior, strong platform-hardening, and well-practiced recovery procedures. Economic analysis also matters.

Process bus adoption can reduce field wiring and create lifecycle value, but those benefits are not automatic; they depend on how reliability, maintenance, spare strategy, and penalties for unserved energy are modeled in the chosen architecture (Diaz et al., 2020; Santos & Zancul, 2023).

## VI. DISTRIBUTED BUSBAR PROTECTION SCHEMES

In a distributed busbar protection scheme, measurement acquisition and some or all protection functions are partitioned among multiple devices, usually at or near bay level. A central coordinator may still exist, but it is no longer the sole concentration point for all intelligence.

Modern distributed schemes commonly rely on bay units, merging units, and peer or hierarchical communications using sampled values, GOOSE, PRP/HSR redundancy, and deterministic engineering models.

This architecture is well aligned with IEC 61850 process bus and is frequently favored in retrofit programs because bays can be digitized incrementally (Teoh et al., 2020; Mathew et al., 2022; Tobar-Rosero et al., 2025).

The principal architectural advantage of distribution is graceful degradation. If one device, link, or bay-level function fails, the entire busbar protection system does not necessarily become blind. The fault may be localized to a subset of the plant, allowing continued service or simplified maintenance. This modularity also supports staged extension.

New bays can often be added with less disturbance to the existing protection population than in a tightly centralized design. For utilities with long asset lives and frequent retrofit constraints, that is an important practical advantage (Santos et al., 2025; Tobar-Rosero et al., 2025).

Distributed schemes can also shorten the physical measurement path by processing signals close to the bay. In hardwired terms this means less extensive secondary wiring; in digital terms it means more localized acquisition and possibly lower exposure to a single point of computational failure.

Industry experience with process-bus-based busbar protection emphasizes that distributed designs fit naturally with sampled-value publishers and bay-oriented commissioning. Testing can often be organized per bay, then coordinated at the zone level, rather than executed as one monolithic platform activity (Teoh et al., 2020; Mathew et al., 2022).

Yet distributed architecture introduces its own costs. Protection quality now depends on correct behavior across multiple devices, engineering files, virtual circuits, and communication subscriptions. Interoperability becomes more challenging, especially in multivendor systems.

Bay additions and maintenance interventions increase configuration-management burden. A device-by-device design can also diffuse responsibility unless utilities establish strict governance over SCL files, firmware baselines, test procedures, and change control.

In other words, distributed architecture improves modularity at the price of systems-integration complexity (Ayello & Lopes, 2023; Bhattacharjee et al., 2022; Chen et al., 2021).

The distributed model therefore favors organizations that are operationally mature in IEC 61850 engineering, multivendor testing, and lifecycle documentation. Where those capabilities are weak, the distributed scheme's theoretical resilience can be undermined by ordinary maintenance errors.

Security in the classical relay sense may remain strong, but security in the practical operational sense may deteriorate if configuration governance is poor.

## VII. CENTRALIZED VERSUS DISTRIBUTED: COMPARATIVE TECHNICAL ANALYSIS

Centralized and distributed busbar protection should not be reduced to a simple binary of “modern” versus “traditional” or “better” versus “worse”. They are two different ways of allocating intelligence, dependency, and risk. Centralization concentrates intelligence and therefore simplifies some forms of coordination and event analysis.

Distribution partitions intelligence and therefore improves modularity and often maintainability. The critical question is where the scheme places its most dangerous failure modes.

For speed, the comparison is nuanced. A centralized algorithm can be extremely fast when deterministic communications, coherent sampling, and stable topology information are available.

However, its performance may be more sensitive to communication and time-distribution defects. Distributed schemes may benefit from local acquisition and shorter logical paths, but protection decision-making can still be delayed if peer coordination or topology exchange is slow or inconsistent.

Consequently, utilities should not compare only nominal trip time; they should compare trip time under degraded conditions such as time-source failure, packet loss, or maintenance bypass.

For selectivity and operational security, both architectures still depend fundamentally on the underlying differential criterion and CT behavior.

Techniques such as alternative generalized alpha-plane protection, superimposed current criteria, and pattern-based approaches attempt to strengthen discrimination under difficult conditions (Vásquez & Silva, 2021; Joband et al., 2023; Sarlak, 2024).

Architecture modifies how measurement errors are aggregated and how supervision is implemented. Centralized systems may be more exposed to artificial spill current created by desynchronization, whereas distributed systems may be more exposed to inconsistent topology or virtual-circuit definitions across multiple nodes.

For lifecycle value, the literature increasingly favors architecture-aware evaluation rather than technology enthusiasm. Digitalization can reduce copper, enhance diagnostics, and support better engineering workflows, but those benefits appear only when supported by interoperability planning, testing discipline, and staff capability.

Multivendor platforms, virtualized IEDs, and centralized PAC systems expand flexibility, yet they also demand stronger engineering management than conventional systems ever required (Bhattacharjee et al., 2022; Santos & Zancul, 2023; Rösch et al., 2024).

| Criterion | Centralized | Distributed |
|---|---|---|
| System visibility | High global visibility in one logic point | Partitioned visibility; coordination required |
| Single-point failure exposure | Higher unless compute and timing are | Lower for device-level failures; more |

| | | |
|---|---|---|
| | strongly redundant | nodes to manage |
| Retrofit flexibility | Often harder in phased retrofits | Usually better for incremental migration |
| Synchronization sensitivity | Typically high | Still significant, but impacts may localize |
| Interoperability burden | Moderate at platform level | Often high across many devices and files |
| Maintenance model | Platform-centric | Device- and configuration-centric |
| Cyber blast radius | Potentially broad | Potentially segmented but harder to govern uniformly |
| Best use cases | Greenfield stations, strong platform engineering, rich analytics | Incremental retrofits, modular expansion, bay-oriented operations |

## VIII. DEPENDABILITY AND SECURITY ASSESSMENT

A useful architecture comparison must distinguish between dependability and security rather than treating "reliability" as a single undifferentiated idea. In protection engineering, dependability refers to correct operation for faults within the intended zone.

Security refers to restraint for external faults, normal load, switching events, or distorted measurements. In digital substations, a second layer must be added: cybersecurity, meaning resistance to malicious interference with measurement, communication, timing, computation, and engineering data (Gaggero et al., 2025; Gaspar et al., 2023).

### 8.1 Dependability for internal faults

Dependability begins with the measurement chain. If bay currents are missing, misassigned, delayed, or corrupted, differential logic can fail to assert for a genuine internal bus fault.

Centralized schemes are especially sensitive to coherent arrival of multi-bay data streams. Song et al. (2020) demonstrate that data desynchronization can create enough error to threaten correct operation unless compensation is implemented.

Time synchronization surveys reinforce this point by showing that process-bus applications have extremely tight timing expectations and that sub-microsecond or microsecond-level integrity is not a luxury but a protection requirement (Liu et al., 2025).

Distributed schemes can improve internal-fault dependability by localizing acquisition and reducing dependence on one central processor, but they also distribute the opportunities for configuration mismatch.

Bay-level misassignment, missing subscriptions, and virtual-circuit inconsistencies can disable differential participation of a single branch and therefore weaken zone coverage.

Recent work on intelligent substation virtual-circuit verification shows why automated checking is increasingly necessary: as the number of IEDs and connections grows, manual verification becomes slow and error-prone (Cao et al., 2024).

Algorithmic innovation also matters. Alternative generalized alpha-plane protection, superimposed current criteria, and Lissajous-based approaches seek to preserve or improve internal-fault sensitivity while resisting difficult transient conditions (Vásquez & Silva, 2021; Joband et al., 2023; Sarlak, 2024).

Data-driven fault diagnosis methods, while not replacements for primary protection, can strengthen post-fault confidence, supervision, and maintenance prioritization (Jiang et al., 2024; Xue et al., 2025).

### 8.2 Operational security against false operation

Operational security is threatened whenever the scheme interprets external-fault distortion or nonfault disturbance as an internal event. CT saturation remains the classic source of trouble, but digital substations add nonclassical threats: desynchronized sampled values, packet loss, duplicate or stale

GOOSE messages, topology-state errors, and engineering-file inconsistencies.

Centralized schemes are vulnerable because they aggregate all streams in one decision point; distributed schemes are vulnerable because inconsistent state across multiple devices can defeat coordinated restraint.

A rigorous security assessment should therefore ask not only "Does the relay restrain for an external fault?" but also "Does it restrain when an external fault occurs during time-source degradation, when one stream is late, when a maintenance bypass is active, or when a topology change is not propagated everywhere?"

This broader question is still underrepresented in many technical papers, which often validate protection functions under nominal network conditions.

The commissioning literature on process-bus-based busbar protection is valuable precisely because it highlights latency, timing, and field-testing metrics that a purely algorithmic paper may omit (Teoh et al., 2020; Mathew et al., 2022).

8.3 Availability, redundancy, and common-cause failure

Availability complements dependability and security by asking how often the scheme is actually capable of protecting the bus as intended. Here redundancy design becomes central.

PRP and HSR architectures are widely used to avoid communication interruption, but redundancy does not eliminate all risk; it can also create common-cause dependencies if channels share firmware defects, engineering errors, or time-distribution assumptions.

Reliability studies of IEC 61850 communication architectures repeatedly show that repair quality, diagnostic coverage, and common-cause failure strongly influence realized performance (Mathebula & Saha, 2022; Muhammad & Saha, 2024).

Centralized schemes need redundancy at compute, network, and timing levels because the blast radius of central failure is large.

Distributed schemes need redundancy plus strong coordination logic because losing a single bay data source may not fail the whole system but can compromise zone completeness. Recent work on economical redundancy schemes for digital substations is useful here because it emphasizes that protection reliability should not be equated with duplicated hardware alone.

Alternative sampled-value sourcing, adjacent backup relationships, and adaptive switching logic can increase resilience without replicating every component in full (Samkari, 2025).

8.4 Cybersecurity as part of protection security

In digital substations, cybersecurity is no longer external to protection quality. A successful cyberattack can create delayed tripping, blocked tripping, false tripping, or hidden impairment of supervision. GOOSE and sampled-value communications are especially important because they operate close to real-time protection functions.

Surveys of smart substation communications and protection-relay cybersecurity show that message spoofing, replay, man-in-the-middle manipulation, denial of service, and unauthorized engineering access are among the most important threat classes (Gaspar et al., 2023; Gaggero et al., 2025).

The cyber exposure of centralized architectures is structurally different from that of distributed architectures. Centralized systems concentrate valuable targets: central processors, engineering repositories, time sources, and virtualization platforms. A compromise there can have wide-area protection consequences. Distributed systems segment some risk, but the number of endpoints rises.

That enlarges the attack surface for credentials, configuration files, firmware drift, and lateral movement. Therefore, "distributed" should not be mistaken for "secure by default". It is secure only if endpoint governance is strong (Silveira et al., 2023; Kabbara et al., 2025).

© JUL 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1719675

The literature increasingly points toward layered protection: IEC 62351-based controls, role-based access control, cryptographic protection of critical traffic where timing allows, anomaly detection for GOOSE and other process-bus traffic, and platform hardening for virtualized IEDs (Shin et al., 2024; Nhung-Nguyen et al., 2024; Alonso et al., 2024).

Machine-learning-based anomaly detection for GOOSE is especially relevant because it addresses the exact traffic class on which many digital protection interactions depend. However, such tools should be treated as supervisory layers, not as substitutes for deterministic engineering controls.

A useful practical conclusion emerges from the cyber literature: the same features that improve engineering flexibility - centralized databases, remote engineering access, virtualization, and multivendor interoperability - also expand the need for cyber governance. Dependability and security should therefore be assessed together, not in separate organizational silos.


Figure 3. Conceptual dependability-security assessment framework used in this review.

## IX. TESTING, COMMISSIONING, AND LIFECYCLE GOVERNANCE

Busbar protection design cannot be validated through simulation alone. Digital substations require extensive FAT, SAT, interoperability testing, virtual-circuit validation, timing verification, and cyber hardening review. This is especially true for busbar protection because it aggregates many bays and often interacts with breaker-failure logic.

Practical experience from process-bus commissioning shows that utilities must measure not only nominal protection behavior but also network latency, timing quality, device failover, and sampled-value consistency under field conditions (Mathew et al., 2022; Teoh et al., 2020).

Hardware-in-the-loop work is also increasingly relevant. HIL studies allow protection functions, communications, and real IEDs to be evaluated under representative disturbance conditions before site deployment.

That is valuable for both centralized and distributed schemes because it reveals behavior under degraded conditions that may not be visible in ordinary desktop studies (Nomandela et al., 2025).

Lifecycle governance is the final, and often underestimated, layer. Configuration control, firmware baseline management, SCL versioning, cybersecurity patch governance, and recurring validation after plant modification are now part of the protection engineer's problem.

The more digital and multivendor the substation becomes, the less acceptable informal documentation practices become. In a distributed architecture poor governance creates fragmented risk; in a centralized architecture it creates concentrated systemic risk.

## X. SYNTHESIS OF KEY FINDINGS

First, centralized busbar protection is strongest where utilities need unified system visibility, advanced coordinated logic, and centralized analytics, and where they can guarantee high-quality communications, timing, cyber controls, and recovery procedures. It is especially attractive for greenfield digital substations and for broader centralized PAC strategies.

Second, distributed busbar protection is strongest where modularity, phased retrofit, localized maintenance, and graceful degradation are more important than complete functional concentration. It suits utilities that already possess mature IEC 61850 engineering and change-management capability.

Third, dependability and security are shaped less by the label "centralized" or "distributed" than by the quality of engineering beneath it.

A poorly synchronized centralized scheme and a poorly governed distributed scheme can both underperform for different reasons. Good architecture does not rescue weak governance; good governance does not fully rescue weak architecture.

Fourth, a hybrid architecture is often the most practical answer. Distributed acquisition close to the bay, deterministic and redundant communications, centralized supervision or analytics where beneficial, and rigorous cyber and configuration governance together provide a more balanced risk profile than either extreme in many real substations.

## XI. RESEARCH GAPS AND FUTURE DIRECTIONS

Several research gaps remain. The first is the shortage of comparative studies that evaluate centralized and distributed busbar protection under the same degraded conditions, including time-source disturbance, packet loss, endpoint compromise, and staged maintenance states. Many papers validate one design in isolation, which is useful but insufficient for architecture choice.

The second gap is limited integration of cyberattack scenarios into protection-performance validation. The cyber literature on digital substations is growing rapidly, but relatively few studies tie cyber events directly to busbar protection dependability and operational security outcomes.

This gap is particularly important for centralized platforms, process-bus timing, and virtualized IEDs (Gaspar et al., 2023; Gaggero et al., 2025; Kabbara et al., 2025).

Third, lifecycle economics deserves more attention. Utilities need better models that combine CAPEX, maintainability, spare strategy, training, outage risk, cyber controls, and obsolescence when comparing centralized and distributed designs. Process bus economics has been studied, but architecture-specific lifecycle trade-offs remain underdeveloped (Diaz et al., 2020).

Fourth, more work is needed on automated verification: virtual-circuit checking, engineering-file consistency validation, time-synchronization health monitoring, and anomaly detection that can operate without compromising deterministic response.

Finally, hybrid and software-defined protection environments require clearer reference architectures so that utilities can compare offerings on a common technical basis rather than on vendor terminology alone.

## XII. CONCLUSION

Busbar protection has entered a new design era. The main protection principle remains differential, but the practical determinants of performance now extend well beyond relay equations. Centralized and distributed architectures distribute intelligence, dependency, and risk in different ways.

Centralized schemes provide elegant global visibility and powerful coordination, but they concentrate timing, software, and cyber risk. Distributed schemes provide modularity and graceful degradation, but they demand stronger configuration governance and multidevice lifecycle control.

The central conclusion of this review is that the choice between centralized and distributed busbar protection cannot be made on algorithmic grounds alone.

It must be made through a combined dependability and security assessment that includes synchronization, redundancy, interoperability, cyber hardening, testability, and maintenance capability. When those factors are explicitly examined, purely architectural preferences become less useful than architecture-governance fit.

For most utilities, the highest-confidence pathway is a hybrid digital busbar protection philosophy: distributed sensing and acquisition, deterministic IEC 61850 communication with PRP/HSR and redundant time sources, clear central supervision where it adds

value, automated configuration verification, HIL-supported validation, and cybersecurity controls aligned with IEC 62351 and defense-in-depth practice. In short, the future of busbar protection is not simply digital. It is digitally disciplined.

REFERENCES

[1] Akbarzadeh, A., Rueda, J. L., Palensky, P., & others. (2024). Two-stage advanced persistent threat (APT) attack on an IEC 61850 power grid substation. International Journal of Information Security. https://doi.org/10.1007/s10207-024-00856-6

[2] Alonso, F., Cilleruelo, I., & De La Torre, A. (2024). Analysis of cryptographic algorithms to improve cybersecurity in the industrial electrical sector. Applied Sciences, 14(7), 2964. https://doi.org/10.3390/app14072964

[3] Ayello, M., & Lopes, Y. (2023). Interoperability based on IEC 61850 standard: Systematic literature review, certification method proposal, and case study. Electric Power Systems Research, 220, 109355. https://doi.org/10.1016/j.epsr.2023.109355

[4] Bhattacharjee, T., Jamil, M., Alotaibi, M. A., Malik, H., & Nassar, M. E. (2022). Hardware development and interoperability testing of a multivendor-IEC-61850-based digital substation. Energies, 15(5), 1785. https://doi.org/10.3390/en15051785

[5] Cao, H., Feng, F., Zheng, A., & others. (2024). Intelligent substation virtual circuit verification method combining knowledge graph and deep learning. Frontiers in Energy Research, 12, 1395621. https://doi.org/10.3389/fenrg.2024.1395621

[6] Chen, L., Li, H., Charton, T., & Zhang, R. (2021). Virtual digital substation test system and interoperability assessments. Energies, 14(8), 2337. https://doi.org/10.3390/en14082337

[7] Diaz, F. F., Guerrero, F. G., & Barandica, A. (2020). Technical-economic evaluation model for a process bus based on IEC 61850. Sustainable Energy, Grids and Networks, 21, 100288. https://doi.org/10.1016/j.segan.2019.100288

[8] Gaggero, G. B., Girdinio, P., & Marchese, M. (2025). Cybersecurity issues in electrical protection relays: A systematic review. Energies, 18(14), 3796. https://doi.org/10.3390/en18143796

[9] Gaspar, J., Cruz, T., Lam, C.-T., & Simões, P. (2023). Smart substation communications and cybersecurity: A comprehensive survey. IEEE Communications Surveys & Tutorials, 25(4), 2456-2493. https://doi.org/10.1109/COMST.2023.3305468

[10] IEC. (2020). IEC 61850-9-2: Communication networks and systems for power utility automation-Part 9-2: Specific communication service mapping (SCSM)-Sampled values over ISO/IEC 8802-3. International Electrotechnical Commission.

[11] IEC. (2020). IEC 62351-6: Power systems management and associated information exchange-Data and communications security-Part 6: Security for IEC 61850. International Electrotechnical Commission.

[12] IEC. (2020). IEC 62439-3: Industrial communication networks-High availability automation networks-Part 3: Parallel redundancy protocol (PRP) and high-availability seamless redundancy (HSR). International Electrotechnical Commission.

[13] Jiang, X., Cao, H., Zhou, C., Ren, X., Shen, J., & Yu, J. (2024). Busbar fault diagnosis method based on multi-source information fusion. Frontiers in Energy Research, 12, 1443570. https://doi.org/10.3389/fenrg.2024.1443570

[14] Joband, M., Homayounifar, S., & Sarlak, M. (2023). A superimposed current based busbar protection scheme using slope degree of grey incidence analysis model. IET Generation, Transmission & Distribution, 17(3), 161-180. https://doi.org/10.1049/gtd2.12671

[15] Kabbara, N., Nait Belaid, M. O., Gibescu, M., Camargo, L. R., Cantenot, J., Coste, T., Audebert, V., & Morais, H. (2022). Towards software-defined protection, automation, and control in power systems: Concepts, state of the art, and future challenges. Energies, 15(24), 9362. https://doi.org/10.3390/en15249362

[16] Kabbara, N., Rueda Torres, J. L., Gibescu, M., & Palensky, P. (2025). A cybersecurity assessment for hybrid virtualized-physical digital substations. Proceedings/technical paper, Delft University of Technology repository.

[17] Kazme, H. Z., Westerlund, P., & Bollen, M. H. J. (2025). Evaluating 5G communication for IEC 61850 digital substations: Historical context and latency challenges. Energies, 18(16), 4387. https://doi.org/10.3390/en18164387

[18] Lima, D. A. C., Bernardon, D. P., Morais, A. P., Oliveira, A. L., Hokama, W. S., Conceição, J. B. R., & Sartori, Â. F. (2022). Review of bus differential protection using IEC 61850. Energies, 15(24), 9537. https://doi.org/10.3390/en15249537

[19] Liu, D., Li, Y., & others. (2024). Strategy for evaluating the status of relay protection equipment for the new generation of intelligent substations. Frontiers in Energy Research, 12, 1342793. https://doi.org/10.3389/fenrg.2024.1342793

[20] Liu, Y., Sun, B., Wu, Y., Zhang, Y., Yang, J., Wang, W., Thotakura, N. L., Liu, Q., & Liu, Y. (2025). Time synchronization techniques in the modern smart grid: A comprehensive survey. Energies, 18(5), 1163. https://doi.org/10.3390/en18051163

[21] Mathebula, V. C., & Saha, A. K. (2022). Reliability of IEC 61850 based substation communication network architecture considering quality of repairs and common cause failures. Protection and Control of Modern Power Systems, 7, 13. https://doi.org/10.1186/s41601-022-00234-1

[22] Mathew, J. M., Hunt, R., Mendez, J., & Smith, T. (2022). Lessons learned from commissioning of IEC 61850-9-2 process-bus-based busbar protection system. Technical conference paper/industry report.

[23] Muhammad, A. M., & Saha, A. K. (2024). A review reliability and availability analysis of IEC 61850 based substation communication architectures. American Journal of Science, Engineering and Technology, 9(3), 175-190. https://doi.org/10.11648/j.ajset.20240903.13

[24] Nhung-Nguyen, H., Girdhar, M., Kim, Y.-H., & Hong, J. (2024). Machine-learning-based anomaly detection for GOOSE in digital substations. Energies, 17(15), 3745. https://doi.org/10.3390/en17153745

[25] Nomandela, S., Mnguni, M. E. S., & Raji, A. K. (2025). Systematic development and hardware-in-the-loop testing of an IEC 61850 standard-based monitoring and protection system for a modern power grid point of common coupling. Energies, 18(19), 5281. https://doi.org/10.3390/en18195281

[26] Rubio, S., Bogarra, S., Nunes, M., & Gomez, X. (2025). Smart grid protection, automation and control: Challenges and opportunities. Applied Sciences, 15(6), 3186. https://doi.org/10.3390/app15063186

[27] Samkari, H. S. (2025). Enhancing substation protection reliability through economical redundancy schemes. Electronics, 14(20), 4097. https://doi.org/10.3390/electronics14204097

[28] Santos, G. R., & Zancul, E. (2023). A framework to assess the impacts of digital electrical substations. Smart Energy, 12, 100125. https://doi.org/10.1016/j.segy.2023.100125

[29] Santos, G. R., Zancul, E., & Rego, E. E. (2025). Pathways to digital substations: A comparative case study. IEEE Latin America Transactions, 23(12), 1297-1304. https://doi.org/10.1109/TLA.2025.11231215

[30] Santos, G. R., Zancul, E., Manassero, G., & Spinola, M. (2024). From conventional to smart substations: A classification model. Electric Power Systems Research, 226, 109887. https://doi.org/10.1016/j.epsr.2023.109887

[31] Sarlak, M. (2024). A Lissajous curve-based method for busbar protection. International Transactions on Electrical Energy Systems, 2024, 8834200. https://doi.org/10.1155/etep/8834200

[32] Shin, S.-H., Kim, J., & others. (2024). Architecture for enhancing communication security with RBAC IoT protocol-based microgrids. Sensors, 24(18), 6000. https://doi.org/10.3390/s24186000

[33] Silveira, P., Silva, E. F., Galletta, A., & Lopes, Y. (2023). Security analysis of digitized substations: A systematic review of GOOSE messages. Internet of Things, 22, 100760. https://doi.org/10.1016/j.iot.2023.100760

[34] Song, M.-H., Kang, S.-H., Lee, N.-H., & Nam, S.-R. (2020). IEC 61850-based centralized busbar differential protection with data desynchronization compensation. Energies, 13(4), 967. https://doi.org/10.3390/en13040967

[35] Teoh, C.-P., Lloyd, G., Richards, S., Newman, P., Qin, H., Hunt, R., Mendez, J., Smith, T., & Abdulla, A. (2020). Process bus busbar protection - A stepping stone towards digital substation. In Proceedings of the 15th International Conference on Developments in Power System Protection (DPSP 2020). IET.

[36] Tobar-Rosero, O. A., Díaz-Mendoza, O. D., Díaz-Vargas, P. A., Candelo-Becerra, J. E., Florez-Célis, H. A., & Quintero-Henao, L. F. (2025). Digital substations: Optimization opportunities from communication architectures and emerging technologies. Sci, 7(2), 63. https://doi.org/10.3390/sci7020063

[37] Vásquez, F. A. M., & Silva, K. M. (2021). Busbar differential protection using an alternative generalized alpha plane. Electric Power Systems Research, 196, 107284. https://doi.org/10.1016/j.epsr.2021.107284

[38] Wu, X., Zhao, H., Xu, W., Pan, W., Ji, Q., & Hua, X. (2024). Fault diagnosis of the distribution network based on the D-S evidence theory Bayesian network. Frontiers in Energy Research, 12, 1422639. https://doi.org/10.3389/fenrg.2024.1422639

[39] Xue, C., Zhang, L., & others. (2025). INFO-RF-based fault diagnosis and analysis method for busbar faults in power systems. Scientific Reports, 15, Article 7402.