Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

An Integrated Lifecycle Framework for Testing, Commissioning, and Reliability Assurance in Modern Substations

Omer Sikander

Tendering & Contracts Manager, Alfanar Projects, Riyadh, Saudi Arabia

Corresponding author: omer.sikander221@outlook.com

Abstract

Modern substations integrate primary plant, intelligent electronic devices, protection and control functions, communication networks, precision timing, supervisory control, and digital process-bus interfaces. Although this integration improves observability and automation, it also creates systemic commissioning risk because defects in settings, wiring, data models, network configuration, time synchronization, or interlocking may remain latent until energization or an actual fault. This study develops the Integrated Testing, Commissioning and Reliability Assurance Framework (ITCRAF) through a structured synthesis of international standards, regulatory guidance, scholarly literature, and documented industry practices. ITCRAF organizes assurance into five lifecycle gates: design assurance, factory acceptance, site acceptance, integrated commissioning and energization, and post-energization reliability assurance. Each gate is linked to accountable roles, mandatory evidence, hold points, test coverage, defect governance, configuration baselines, and reliability indicators. An illustrative 132/33 kV digital-substation scenario demonstrates how requirements traceability, risk-priority assessment, end-to-end protection testing, IEC 61850 configuration validation, readiness scoring, and controlled handover can be integrated without claiming empirical project outcomes. A prospective case-study protocol is also proposed to assess framework feasibility, reviewer agreement, assurance performance,

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

configuration control, scoring sensitivity, and early operational outcomes during a future pilot and 12-month follow-up. The principal contribution is an auditable lifecycle model that converts commissioning evidence into an initial reliability baseline for operations and maintenance. The framework can support utilities, engineering-procurement-construction contractors, original equipment manufacturers, and regulators in governing interface risk during grid expansion, renewable-energy integration, and digital-substation deployment.

Keywords: Digital Substation; IEC 61850; Protection-System Testing; Commissioning Readiness; Reliability Assurance

1. Introduction

Electricity grids are becoming more extensive, digitally connected, and operationally interdependent. The International Energy Agency identifies modern, smart, and expanded grids as essential to secure energy transitions because electrification and renewable generation place additional demands on transmission and distribution infrastructure [1]. Its recent transmission-grid analysis further emphasizes the scale, coordination, and delivery challenges involved in building future network capacity [15]. At project level, this transformation is visible in modern substations, where conventional primary equipment is integrated with multifunction protection relays, station and process buses, supervisory systems, gateways, precision time sources, engineering workstations, and remote-control interfaces.

The value of this technology depends on correct engineering and dependable commissioning. Protection systems must detect abnormal conditions and isolate faulted elements selectively and rapidly. Automation must execute permitted sequences while blocking unsafe operations. Measurements, alarms, status indications, and control commands must map correctly between field devices and control centers. Communication-assisted schemes must meet performance

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

requirements under normal and degraded network conditions. These obligations cannot be demonstrated by isolated equipment tests alone.

IEC 61850 addresses interoperability for power-utility automation through standardized data models, Substation Configuration Language (SCL), communication services, and protocols [2,3]. The standard enables multi-vendor digital architecture, but it also shifts substantial engineering content into configuration files, logical-node models, message subscriptions, network design, and time synchronization. Consequently, testing must verify not only individual devices but also the implemented system, interfaces, data flows, failure behavior, and configuration baseline.

Protection-system performance is a reliability concern rather than a narrow commissioning concern. The North American Electric Reliability Corporation notes that protection-system mis operations are associated with the propagation of major system failures and therefore require systematic information collection, analysis, and correction [4]. Its PRC-004-6 standard further emphasizes dated evidence, event review, and correction of identified causes [5]. Although these requirements apply within a specific regulatory jurisdiction, the underlying principle is broadly relevant: reliable protection depends on demonstrable evidence, disciplined analysis, and closed corrective actions.

Saudi Arabia provides a strategically important application context because electricity-sector reform seeks to improve grid reliability, network efficiency, renewable-energy integration, and distribution-network digitalization [6]. The Ministry of Energy also states that renewables are intended to constitute around 50% of the energy mix used to produce electricity by 2030 [7]. Delivering this transition requires more than constructing new assets: transmission and distribution projects must enter service with verified protection, automation, communication, cybersecurity, and configuration baselines. As the number of digitally enabled substations and renewable interconnections increases, inconsistent commissioning evidence can become a portfolio-level

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

reliability risk. A repeatable lifecycle assurance framework is therefore directly relevant to the dependable grid expansion required by Vision 2030.

This study addresses the practical gap between equipment-oriented testing and lifecycle reliability governance. It proposes an Integrated Testing, Commissioning and Reliability Assurance Framework (ITCRAF) that organizes evidence from design through operation. The paper asks three research questions:

(RQ1) Which technical and governance controls are required at each substation assurance gate?

(RQ2) How can project test evidence become an operational reliability baseline?

(RQ3) How can readiness and residual risk be represented without creating a false impression of precision?

The study contributes a structured lifecycle, a traceability model, a risk-based readiness index, a reliability scorecard, and an illustrative digital-substation application. It does not claim causal improvement from field data. Instead, it provides a transparent technical artifact that can be validated through expert review, pilot implementation, and longitudinal project evidence.

The novelty of ITCRAF lies in integrating four assurance layers that are usually managed separately: technical verification, evidence traceability, configuration integrity, and post-energization reliability feedback. Existing standards and practices address important parts of this lifecycle, but they do not by themselves provide a single decision model that links a requirement to its risk, test evidence, defect disposition, as-left configuration, energization authority, and subsequent operational learning. ITCRAF contributes this missing chain while retaining hard safety and protection gates that cannot be overridden by aggregate readiness scores.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

2. Literature Review

2.1 Substation automation and digital architecture

IEC 61850 is a leading interoperability technology for power-utility automation. Its architecture combines semantic data models, SCL-based engineering, standardized communication services, and security support through IEC 62351 [2]. The current consolidated IEC 61850-5 edition defines communication requirements for utility-automation functions and device models [3]. IEC 61850-10 specifies conformance testing for client, server, sampled-value devices, engineering tools, and GOOSE performance, while IEC TR 61850-10-3 addresses functional verification of deployed IEC 61850 systems [16,17]. Product conformance improves interoperability evidence but does not prove that a particular engineered application, configuration, logic, or end-to-end scheme is functionally correct.

Digital substations replace or supplement conventional secondary copper circuits with GOOSE messages, sampled values, communication networks, and synchronized data. Practical projects report testing requirements covering network behavior, time synchronization, sampled values, GOOSE-based protection, interlocking, and contingency simulation [8]. Applicable process-bus assurance should verify merging-unit configuration, sampled-value subscriptions, quality attributes, sampling and time alignment, loss or degradation behavior, network redundancy, and recovery. IEC/IEEE 61850-9-3 provides the precision-time profile for power-utility automation, and IEC 62351-6 defines security mechanisms for IEC 61850-related communication profiles [18,19]. This broadens commissioning from physical continuity and injection testing to cyber-physical verification across devices, applications, networks, timing sources, and security controls.

Centralized protection and control introduce additional architectural choices. IEEE C37.300-2024 addresses centralized protection and control systems, including architecture, reliability, maintainability, testing, installation, commissioning, troubleshooting, and maintenance [9]. The

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

guide reinforces the need to assess system architecture and lifecycle support, not merely the correctness of individual protection functions.

2.2 Testing and commissioning practices

Testing is performed at multiple levels. Type and conformance testing establish product or implementation characteristics. Factory acceptance testing verifies the assembled system against approved specifications before shipment. Site acceptance testing confirms installation, interfaces, wiring, communications, settings, and functionality at site. Integrated commissioning establishes that the complete system performs under normal, abnormal, and contingency conditions. Energization authorization confirms that technical evidence, safety clearances, operational ownership, residual-risk acceptance, and release approvals permit the controlled transition into service. Maintenance testing subsequently verifies that protection and control capabilities remain dependable after configuration changes, aging, firmware updates, and operational events.

Digital relay testing must cover more than calibrated pickup values. IEC 60255-1:2022 establishes common requirements and tests for measuring relays and protection equipment, including distributed protection schemes and communication interfaces [24]. Industry guidance also emphasizes settings, logic, inputs/outputs, communications, documentation, and as-found/as-left files [10]. Microprocessor-relay self-diagnostics do not prove correct settings, external wiring, application logic, trip paths, or coordinated interfaces. Independent settings comparison and end-to-end tests are therefore required where scheme performance depends on multiple devices, tele protection channels, or distributed logic.

Apostolov describes efficient maintenance testing for IEC 61850 Edition 2 environments and highlights isolation, test modes, remote testing, security, and outage reduction [11]. Recent work on commissioning digital substations similarly argues for structured approaches that combine configuration knowledge with testing and secure start-up [12]. The literature therefore supports

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

testability by design, virtual isolation, repeatable automated tests, and controlled configuration management.

2.3 Reliability assurance and maintenance

Commissioning creates the first verified system baseline, but reliability assurance continues throughout operation. Reliability-centered maintenance prioritizes functions and failure consequences rather than applying uniform maintenance intervals. In substation environments, this principle can combine equipment health, failure modes, criticality, protection-system history, diagnostics, disturbance records, and outage consequences. Reliability-based maintenance research similarly seeks to allocate attention according to component importance and system impact [13]. NERC PRC-005-6 provides a dedicated maintenance-program reference for protection systems, automatic reclosing, and sudden-pressure relaying [20], while ISO 55001:2024 grounds the transition in lifecycle asset-management governance, control of change, data, and documented information [21]. These sources are jurisdictionally distinct and are used as transferable evidence principles rather than universal Saudi compliance obligations.

Protection-mis operation analysis demonstrates the need for feedback. NERC collects categorized mis operation information and uses it to examine regional trends [4]. PRC-004-6 requires owners to determine whether protection-system components caused a mis operation and to maintain supporting evidence [5]. A mature utility can extend this principle into a closed loop: operating events update failure libraries, test procedures, settings governance, training, spares strategy, and future project specifications.

The literature remains fragmented across four domains. Standards define interoperability and technical requirements; project practices explain test execution; reliability regulation emphasize event evidence and corrective action after operation; and asset-management research prioritizes maintenance using criticality and consequence. None of these streams, when applied alone, preserves a complete and auditable chain from an approved design requirement to risk

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

classification, test evidence, defect disposition, energization release, as-left configuration, and operational reliability feedback. This unresolved integration problem is the specific research gap addressed by ITCRAF.

Table 1. Synthesis of evidence streams and their implication for lifecycle assurance

Evidence stream	Primary contribution	Limitation when used alone	ITCRAF response
IEC 61850 and related standards	Interoperable models, engineering language, communication and system requirements	Compliance does not prove the deployed application is correct	Validate models, files, subscriptions, timing and application behavior
Protection testing practice	Functional and end-to-end verification	May become device-centric or procedure-centric	Link tests to requirements, risks and acceptance evidence
Reliability regulation	Event analysis, evidence and corrective action	Often begins after operation	Use commissioning evidence as the initial reliability baseline
Reliability-centered maintenance	Criticality and consequence-based maintenance	Depends on reliable asset and failure data	Connect asset register, test results, events and maintenance strategy
Project governance	Roles, hold points and approvals	Can become documentary rather than technical	Use evidence-based stage gates and residual-risk acceptance

3. Methodology

3.1 Study design

This research used a technical-framework development design to construct a transparent and auditable assurance artifact rather than estimate a population effect. The procedure comprised seven linked phases: identifying authoritative evidence; extracting technical, governance, safety, configuration, and reliability requirements; coding recurring controls; mapping each control to the lifecycle stage at which it most effectively prevents or detects failure; defining mandatory evidence and hold points; demonstrating the resulting model through an illustrative digital-substation scenario; and specifying a prospective case-study protocol for future pilot validation and longitudinal follow-up. The final framework was checked for internal consistency by confirming that every proposed gate produced evidence required by a later gate or by operational reliability assurance. The prospective protocol was designed to evaluate feasibility, reviewer agreement,

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

defect-detection yield, configuration control, score sensitivity, implementation burden, and early operational outcomes without treating the illustrative scenario as empirical validation.

Authoritative sources were prioritized in the following order: international standards and official standards summaries; regulatory and reliability guidance; official government energy-policy sources; peer-reviewed or publisher-indexed scholarly work; and documented industry case material. A source was included when it directly informed at least one framework construct: substation automation, protection testing, commissioning, IEC 61850 engineering, system integration, reliability assurance, mis operation analysis, or utility maintenance. Sources were excluded when bibliographic details could not be verified, the material repeated a higher-authority source without adding technical insight, or no direct relationship to a framework construct could be established. Requirements and recurring controls were compared across source types so that no single regulatory jurisdiction, vendor practice, or technical discipline determined the complete framework.

3.2 Analytical procedure

The analytical procedure contained six steps:

1. Extract requirements and recurring controls from the selected evidence.
2. Code each control as technical, process, evidence, governance, safety, configuration, or reliability related.
3. Map controls to the lifecycle stage where failure prevention is most effective.
4. Define minimum gate evidence and explicit hold points.
5. Develop a risk-based readiness calculation that separates completion from unresolved critical risk.
6. Apply the framework to an illustrative 132/33 kV digital-substation scenario to demonstrate the readiness calculation, and specify a prospective case-study protocol for evaluating the framework during a future pilot and post-energization follow-up.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

3.3 Risk and readiness measures

Failure modes are prioritized using a conventional Risk Priority Number (RPN): RPN = Severity × Occurrence × Detection Difficulty. The three factors are ordinal review scales, not calibrated probability or consequence measures; therefore, RPN is used only to rank and discuss failure modes within a defined project context, and arithmetic differences must not be interpreted as proportional differences in actual risk. Severity (S) is anchored as 1 = negligible documentary effect, 2 = minor functional degradation without loss of required protection, 3 = material operational degradation or limited outage exposure, 4 = major loss of protection/control capability or significant outage exposure, and 5 = safety-critical, protection-critical, regulatory, or potentially widespread consequence. Occurrence (O) is anchored as 1 = exceptional under controlled conditions, 2 = unlikely but credible, 3 = occasional, 4 = recurring, and 5 = frequent/systemic based on applicable organizational evidence. Detection difficulty (D) is anchored as 1 = almost certain detection by routine checks, 2 = high detectability, 3 = moderate detectability requiring a targeted test, 4 = low detectability without integrated testing, and 5 = latent until energization, fault, or abnormal operation. These anchors are provisional and require pilot calibration. Any safety-critical, protection-critical, regulatory, or energization-blocking failure remains Category A and a hard gate irrespective of RPN. During validation, independent reviewers shall score S/O/D and defect class before consensus, with pre-consensus agreement reported using scale-appropriate reliability statistics.

The Commissioning Readiness Index (CRI) is a weighted completion measure across assurance domains: $CRI = \Sigma(w_i \times c_i)$, subject to $\Sigma w_i = 1$. For each domain, c_i equals verified earned evidence points divided by total applicable evidence points in the approved domain register. The register must identify the governing requirement, test or evidence item, assigned point value, acceptance criterion, verifier, and status. A passed and independently verified item earns full points; an incomplete or unexecuted item earns zero; a failed item earns zero until corrective action and

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

successful retest are verified; a successfully retested item earns full points while its initial failure remains in first-pass-yield reporting; and a waived item earns zero unless the designated technical and asset authorities document justification, residual risk, compensating controls, accountable approval, and a review or expiry date. Partial credit is permitted only where the approved evidence register defines objective milestones before execution. Not-applicable items require documented technical approval and are removed from the denominator; the remaining domain weights are renormalized proportionally so that their sum remains 1. Profile-specific weights may instead be approved before assessment for conventional, station-bus, process-bus, or centralized architectures. The illustrative weights are design and settings assurance 20%, primary equipment and secondary circuits 20%, protection and control functions 25%, automation and communications 15%, safety and energization controls 10%, and documentation and operational handover 10%. CRI is a transparency mechanism, not a substitute for engineering judgment or risk acceptance. Readiness requires an illustrative CRI of at least 90.0%, zero open Category A defects, and approval of every mandatory hold point. The threshold, weights, point values, and Category B treatment are author-developed design parameters requiring expert validation and sensitivity analysis across alternative weights and thresholds.

Defects are classified as Category A (unsafe, protection-critical, regulatory, or energization-blocking), Category B (material functional or reliability deficiency with an approved correction plan), or Category C (minor documentary or cosmetic issue that does not undermine safe operation). The discipline lead proposes the classification, the commissioning manager records it, and the designated technical authority confirms Category A and disputed classifications. The asset owner or formally delegated release authority accepts documented residual risk. A waiver must identify the affected requirement and evidence, technical justification, residual risk, compensating controls, accountable approvers, owner, due date, and expiry or review trigger. Category A defects cannot be waived for energization. Approved changes trigger impact analysis, mapping to affected

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

requirements and test cases, regression testing, approval, deployment confirmation, baseline update, and retention of a tested rollback package.

3.4 Scenario and limitations

The application is an illustrative scenario for a new 132/33 kV substation with two power transformers, line and transformer protection, IEC 61850 station-bus communication, GOOSE interlocking and tripping, SCADA integration, disturbance recording, redundant Ethernet, and gateway communication to a control center. All requirements counts, defect counts, completion ratios, risk ratings, readiness values, and operational conditions presented in the scenario are hypothetical and are used only to demonstrate the method. No confidential project record, human participant, or personal data was used. Accordingly, institutional ethical approval was not required for this conceptual technical study.

4. Results

4.1 Integrated Testing, Commissioning and Reliability Assurance Framework

ITCRAF contains five assurance gates. Each gate closes a different class of uncertainty and produces evidence required by the next stage. The sequence is intentionally cumulative: later testing does not compensate for weak requirements, uncontrolled settings, incomplete design review, or missing configuration baselines.

Table 2. ITCRAF lifecycle and evidence flow (author-developed)

Gate 1	Gate 2	Gate 3	Gate 4	Gate 5
Design assurance	Factory acceptance	Site acceptance	Integrated commissioning and energization	Operational reliability assurance
Requirements baseline	Verified system build	Verified installation	Approved operational release	Closed feedback and maintained baseline

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

Gate 1: Design and settings assurance

Gate 1 verifies that the intended system is testable, coordinated, and traceable. Required evidence includes approved single-line diagrams, protection philosophies, grading and settings studies, instrument-transformer requirements, communication architecture, time-synchronization design, I/O lists, signal matrices, interlocking narratives, cybersecurity zoning, SCL governance, test specifications, and a traceability matrix. Attention is given to boundaries between the utility, EPC contractor, OEMs, telecommunications provider, and control-center team.

Gate 2: Factory acceptance

Gate 2 validates the assembled protection, automation, control, and communication solution before deployment. FAT should include device configuration, logic validation, measurement scaling, alarm and indication mapping, GOOSE publications and subscriptions, sampled-value quality and degradation scenarios where applicable, network redundancy, time synchronization, gateway mapping, HMI displays, conformance evidence, user and role authorization, secure remote access, network segmentation, security logging, service and interface hardening, backup/restore, failover behavior, and configuration-file consistency. Product conformance evidence is reviewed separately from application and system correctness. Deviations are recorded against unique defect identifiers, and the released configuration package becomes a controlled site baseline.

Gate 3: Site acceptance

Gate 3 confirms correct installation and site integration. It covers primary-equipment results, insulation and grounding checks, current-transformer and voltage-transformer polarity and ratio, cable continuity, trip-circuit supervision, DC systems, wiring, input/output points, panel inspections, communication links, network topology, precision-time sources, control-center interfaces, and verification that the deployed configuration matches the approved site baseline. As-left drawings and settings files are captured after approved corrections.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

Gate 4: Integrated commissioning and energization

Gate 4 proves functional performance across equipment and organizational boundaries. Testing includes secondary and primary injection where applicable, end-to-end line-protection schemes, breaker-failure logic, intertripping, transformer differential and restricted-earth-fault schemes, bus protection, autoreclosing, synchrocheck, interlocking, local and remote control, SCADA indications, sequence-of-events recording, disturbance recording, communication degradation, redundant-path failover, loss of the time source, and restoration procedures. Energization requires approved switching programs, safety clearances, transfer of operational ownership, emergency contacts, rollback criteria, and formal authorization by the designated release authority.

Gate 5: Post-energization reliability assurance

Gate 5 converts project evidence into an operational baseline. The asset register is reconciled with installed equipment; approved settings, SCL, gateway/HMI/network files, firmware, cryptographic hashes, approval state, deployment confirmation, and rollback packages are archived; and maintenance tasks are assigned by criticality under the applicable maintenance program [20,21]. Alarms, disturbance records, misoperations, failures to operate, incorrect operations, secure restraints, defects, waivers, and configuration deviations are cause-coded and reviewed. Material network, settings, firmware, topology, or cybersecurity changes trigger impact analysis and regression testing. Future events and near misses update test libraries, maintenance plans, competency requirements, and design standards.

Table 3. Minimum assurance evidence by lifecycle gate

Gate	Minimum evidence	Primary approval question
1. Design	Approved studies, architecture, narratives, I/O, SCL plan, traceability matrix	Is the intended system correct, coordinated and testable?
2. FAT	Executed procedures, results, defects, released files, backups	Does the assembled system satisfy approved requirements?
3. SAT	Installation records, field test results, interface checks, as-left files	Has the system been installed and integrated correctly?

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

4. Commissioning	End-to-end evidence, contingency tests, open-item register, release certificate	Can the complete system be energized and operated safely?
5. Reliability	Asset baseline, maintenance plan, event feedback, change records	Will the verified condition be sustained and improved?

4.2 Traceability and configuration control

The proposed traceability chain is Requirement → Design artifact → Risk → Test case → Test result → Defect/waiver → As-left configuration → Operational asset. This chain allows a reviewer to determine why a test exists, which requirement it demonstrates, what evidence was produced, and whether the final configuration matches the tested state. Every protection-settings file, logic file, SCL file, gateway database, HMI file, and network-configuration file should carry a unique version, approver, cryptographic hash or other controlled identifier, approval status, deployment confirmation, effective date, and tested restoration copy.

Table 4. Example traceability records

Requirement	Risk if unmet	Verification	Acceptance evidence
Transformer differential trips designated breakers	Failure to clear internal transformer fault	Secondary injection and trip-path test	Time-stamped test report and event record
GOOSE interlocking blocks unsafe disconnector operation	Unsafe switching or equipment damage	Positive and negative logic tests	IED event logs and witnessed checklist
Redundant network maintains critical messaging after single failure	Loss of protection/control communications	Link-failure and recovery test	Network capture and alarm/event record
Control-center indication matches field status	Incorrect operator decision	Point-to-point and end-to-end SCADA test	Signed signal matrix
Approved settings equal as-left settings	Uncoordinated or unintended operation	Automated comparison and checksum	Approved comparison report

4.3 Risk register and acceptance gates

Table 5. Illustrative commissioning risk assessment. S = Severity; O = Occurrence; D = Detection Difficulty; RPN = Risk Priority Number.

Failure mode	S	O	D	RPN	Required control	Gate

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

Incorrect CT polarity to differential relay	5	2	3	30	Polarity test plus stability and operate test	SAT
Unapproved relay settings loaded	5	2	4	40	Controlled import, checksum and independent comparison	FAT/SAT
Missing GOOSE subscription	5	2	3	30	SCL validation and end-to-end message test	FAT
Time synchronization unavailable	3	3	2	18	Normal, loss and recovery tests with alarm validation	FAT/SAT
SCADA control mapped to wrong bay	5	2	3	30	Two-person point-to-point verification	SAT
Open trip circuit at energization	5	2	2	20	Trip-circuit supervision and direct trip-path test	Commissioning

Although the calculated scores are moderate, several items remain protection critical. This illustrates why arithmetic prioritization must be combined with hard gates. A low occurrence rating cannot justify energization when the consequence is unsafe switching or failure to clear a fault.

4.4 Measurement definitions and governance rules

Requirements coverage (%) = applicable approved requirements with at least one verified test or inspection result divided by total applicable approved requirements × 100; it is reported separately from executed-test pass rate, which equals passed executed test cases divided by all executed test cases × 100. First-pass yield (%) = test cases accepted on their first controlled execution divided by all test cases first executed in the reporting period × 100; a later successful retest does not revise the original first-pass result. Configuration-baseline compliance (%) = verified in-scope configuration items whose file hash or controlled identifier, version, approval state, and deployed state match the approved baseline divided by all in-scope items examined × 100; protection-critical or security-critical deviations are always reported individually. Alarm-response performance reports time to acknowledgement and time to technical closure by alarm class. Critical-defect closure time is measured from formal identification to verified closure. Forced outages are attributed to commissioning or configuration only after documented event review establishes a defensible causal contribution. Protection performance is reported as dependable correct operation,

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

secure restraint, failure to operate, incorrect operation, and unresolved event count rather than a single aggregate rate.

4.5 Commissioning readiness scorecard

Table 6. Illustrative Commissioning Readiness Index

Domain	Weight	Verified completion	Weighted score
Design and settings assurance	0.20	0.98	0.196
Primary equipment and secondary circuits	0.20	0.95	0.190
Protection and control functions	0.25	0.92	0.230
Automation and communications	0.15	0.88	0.132
Safety and energization controls	0.10	1.00	0.100
Documentation and operational handover	0.10	0.85	0.085
Total CRI	**1.00**		**93.3%**

The illustrative CRI is reported as 93.3%, not as evidence of measurement precision. Under the proposed rule, this value indicates conditional readiness only when no Category A defect remains open and every mandatory hold point has been signed. The lower completion values for automation and communications (88%) and documentation and operational handover (85%) identify domains requiring management attention, but they do not authorize bypassing critical controls. These percentages correspond to completion ratios of 0.88 and 0.85 in Table 6. No claim is made that a high CRI predicts lower outage or misoperation rates. Future validation must test sensitivity to alternative domain weights and readiness thresholds before any organization adopts decision limits.

4.6 Illustrative 132/33 kV digital-substation application

The scenario begins with 124 traceable requirements distributed across protection, control, communications, primary equipment, safety, cybersecurity, SCADA, and documentation. During design review, six interface ambiguities are identified, including ownership of control-center

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

testing, time-source redundancy, and the boundary between OEM SCL files and the system integrator's final system configuration description. Closing the ambiguities before FAT prevents them from becoming site disputes.

At FAT, the team executes device, logic, messaging, network, HMI, gateway, and failover tests. Three Category B defects are recorded: inconsistent alarm naming, an incorrect GOOSE quality-handling condition, and incomplete time-loss alarming. The released baseline is updated only after retest. At SAT, wiring, CT/VT circuits, trip paths, DC supplies, communications, and point lists are verified. One incorrect SCADA mapping is identified and corrected before integrated commissioning.

Integrated commissioning tests the complete trip chains and operating sequences. The test set includes transformer differential, overcurrent and earth-fault functions, breaker failure, intertripping, synchrocheck, interlocking, remote control, loss of one network path, loss and restoration of time synchronization, control-center indications, disturbance retrieval, and emergency restoration. Evidence is linked to requirements and retained with as-left settings and configuration files.

At readiness review, the illustrative CRI is 93.3%, no Category A defect is open, and remaining Category C documents have owners and due dates. The release authority approves energization subject to a defined early-life monitoring period. During handover, the operational team receives the asset register, drawings, files, test evidence, defect history, maintenance tasks, backups, access controls, and event-review procedure. The result is not a claim of quantified reliability improvement; it is a demonstrable chain of assurance that can later be compared with actual faults, alarms, failures, and maintenance outcomes.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

4.7 Operational reliability scorecard

Table 7. Proposed post-energization reliability indicators

Indicator	Purpose	Initial data source	Interpretation
Protection performance outcomes	Monitor dependable and secure operation	Event and disturbance reviews	Trend with cause coding, not as a stand-alone target
Unresolved critical defects	Prevent normalization of risk	Defect register	Must be zero at energization
Configuration-baseline compliance	Detect unauthorized or undocumented change	Periodic file comparison	Exceptions require investigation
Test first-pass yield	Identify recurring engineering or installation weaknesses	FAT/SAT database	Use by subsystem and supplier
Trip-circuit and communication alarm response	Measure readiness to correct latent failures	Alarm logs and work orders	Track time to acknowledge and close
Forced outage and failure recurrence	Assess reliability impact	Outage and maintenance system	Link events to failure modes and corrective action
Settings review completion	Maintain coordination after network change	Protection governance register	Triggered by defined system changes

5. Discussion

5.1 Technical interpretation

The results answer the three research questions through a single assurance chain. For RQ1, the five gates specify technical controls, accountable roles, evidence, and hold points required from design through operation. For RQ2, the traceability model and controlled as-left configuration convert project test records into an operational asset and reliability baseline. For RQ3, the CRI provides a transparent completion measure, while Category A defects and mandatory hold points remain non-negotiable constraints that prevent numerical scoring from concealing unacceptable residual risk. The illustrative scenario demonstrates internal application of these mechanisms but does not establish empirical effectiveness.

The approach is consistent with IEC 61850's lifecycle orientation. IEC describes interoperability through common models, SCL engineering, communication services, and security support [2]. The implication is that configuration artifacts are operational assets. A tested relay file without the

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

matching SCL, gateway mapping, network configuration, and approved logic cannot fully represent the tested system.

The framework also addresses the limits of self-diagnostics. Digital devices can detect internal problems, yet they cannot independently prove that the application, wiring, settings, external trip circuit, communications, or coordinated scheme is correct. This is why end-to-end verification and contingency testing remain necessary [8,10].

5.2 Reliability and governance implications

ITCRAF treats the energization decision as a governed risk acceptance rather than a ceremonial milestone. The CRI provides visibility of completion, while hard gates prevent numerical aggregation from concealing critical defects. This distinction is important because weighted indices can create false confidence if severe issues are diluted by many completed low-risk tasks.

The post-energization gate operationalizes the feedback principle found in protection-misoperation governance [4,5]. Event records, test results, defects, and corrective actions should update future procedures and specifications. In this way, commissioning becomes the first cycle of reliability management rather than the last cycle of construction.

The framework supports clearer accountability. The design authority owns the technical requirements; the commissioning manager controls procedures and evidence; protection engineers approve settings and functional results; network specialists validate communications; operations controls switching and acceptance; safety authorities control permits; and the asset owner accepts residual risk. Organizations may combine roles, but responsibilities should remain explicit.

5.3 Saudi Vision 2030 relevance

Saudi electricity-sector reform aims to enhance grid reliability, improve efficiency, enable renewable generation, and digitize distribution networks [6]. The National Renewable Energy Program is intended to diversify the energy mix, with renewables expected to represent around

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

50% of electricity production by 2030 [7]. ITCRAF translates these strategic objectives into project-level assurance mechanisms: requirements traceability supports accountable delivery; integrated protection and communication testing reduces latent interface risk; controlled configuration baselines support dependable digital operations; and post-energization indicators create feedback for reliability improvement. The framework does not by itself demonstrate national-level outcomes, but it identifies measurable project evidence through which substation programs can contribute to Vision 2030 implementation.

Renewable integration introduces changing power flows, inverter-based resources, new interconnection-protection requirements, expanded telecommunications, and more frequent network reconfiguration. Region-specific research has examined the reliability implications of renewable expansion in Saudi Arabia using indices such as loss-of-load expectation and loss-of-energy expectation [14]. ITCRAF complements generation-adequacy analysis at the project-delivery layer: it provides evidence that the substations, protection systems, communication paths, control-center interfaces, and configuration baselines through which new resources connect have been verified before energization and remain governed after handover. This distinction positions the framework as an implementation bridge between system-level energy-transition planning and asset-level operational readiness.

For Saudi utilities and EPC programs, ITCRAF can be localized through a national implementation profile. Global technical evidence should be mapped separately from jurisdiction-specific obligations. The profile should map each gate to the Saudi Arabian Grid Code, applicable utility requirements, approved-equipment rules, competency and release authorities, and the NCA Operational Technology Cybersecurity Controls (OTCC-1:2022) [22,23]. Cybersecurity commissioning should include role-based access, secure remote access, segmentation, logging, backup/restore, configuration integrity, and unused-service control. Localization should retain five non-negotiable principles: end-to-end requirements traceability, independent verification of

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

protection-critical functions, controlled as-left baselines, hard energization gates for unresolved critical risk, and operational feedback into future specifications and tests.

5.4 Implementation roadmap

Table 8. Proposed organizational implementation roadmap

Stage	Actions	Deliverable
1. Define	Approve lifecycle, defect classes, roles and mandatory hold points	Commissioning governance standard
2. Standardize	Create requirement, test, evidence and handover templates	Controlled template library
3. Digitize	Implement traceability and configuration repositories	Searchable assurance record
4. Pilot	Apply to one substation and perform independent review	Validated pilot lessons
5. Scale	Train teams and integrate supplier requirements	Portfolio deployment
6. Improve	Use events, failures and audit findings to revise controls	Closed reliability feedback loop

5.5 Prospective case study for framework validation

A prospective case-study validation protocol is proposed for one new or substantially refurbished transmission or distribution substation before portfolio-wide adoption. The protocol should begin before Gate 1 and continue through at least 12 months of post-energization operation so that construct usability, implementation burden, decision consistency, defect-detection yield, and early operational outcomes can be examined. The pilot case must be described by voltage level, conventional, station-bus or process-bus architecture, distributed or centralized protection arrangement, project complexity, principal suppliers, and applicable regulatory profile. No project has yet been enrolled under this protocol, and no validation findings are reported in this manuscript. The protocol therefore does not convert the illustrative 132/33 kV scenario into empirical evidence.

At baseline, the case-study team should freeze the approved requirements register, architecture, roles, evidence register, scoring anchors, defect-classification rules, planned tests, and comparison

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

period. At each gate, two suitably qualified reviewers should independently assess applicable evidence, S/O/D ratings, defect classifications, completion ratios, hold-point status, waivers, reviewer effort, and unresolved disagreements before consensus. Pre-consensus agreement should be reported using statistics appropriate to ordinal scores and categorical classifications. All deviations, retests, waivers, configuration changes, and release decisions should retain time-stamped links to the governing requirement and deployed baseline.

Table 9. Prospective case-study validation measures

Validation domain	Measure	Evidence and timing
Feasibility	Reviewer effort, training time, evidence-preparation effort, unresolved questions, and implementation burden	Time logs and structured feedback at each gate
Decision reliability	Pre-consensus agreement for S/O/D ratings, defect classifications, applicability decisions, and hold-point readiness	Independent reviewer records before consensus
Assurance performance	Requirements coverage, executed-test pass rate, first-pass yield, defects by gate and category, defect-detection yield, retests, waivers, and closure time	Requirements, test, defect, and waiver registers through energization
Configuration control	Baseline compliance, unauthorized deviations, change-impact completeness, regression-test completion, and rollback readiness	Approved and deployed configuration records at FAT, SAT, energization, and follow-up
Operational outcomes	Dependable correct operations, secure restraints, failures to operate, incorrect operations, alarm-response time, early-life failures, forced outages, and repeat defects	Event, disturbance, maintenance, and outage reviews at 3, 6, and 12 months
Score sensitivity	Readiness classification under alternative CRI weights and thresholds	Prespecified sensitivity analysis after the energization decision is locked

Analysis should first test feasibility and reviewer consistency, then examine whether the framework detects material defects earlier and maintains a verifiable configuration baseline. Where a comparable completed project or matched conventional project is available, descriptive comparisons may be made after accounting for voltage level, architecture, project complexity, and supplier capability; such comparison should not be described as causal evidence unless the design

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

and sample support that inference. The case-study report should publish the protocol, missing data, deviations, negative findings, administrative burden, and all prespecified outcome definitions. Validation would support refinement of ITCRAF but would not establish a universal readiness threshold or prove reliability improvement from a single project.

5.6 Limitations and future research

This study is conceptual and scenario-based; it does not establish that ITCRAF reduces outages, defects, costs, or schedule duration. The CRI weights, readiness threshold, defect categories, and scenario values are design proposals rather than validated coefficients. The prospective case-study section is a protocol for future validation, not a report of completed field implementation, and no pilot observations or longitudinal outcomes are presented. Construct validity may be limited because broad concepts such as readiness and reliability are represented through proposed evidence and indicators. External validity is also limited because standards, regulatory guidance, scholarly literature, and industry cases originate from jurisdictions and organizations with different architectures, governance models, and operating conditions. Finally, the illustrative application and unexecuted validation protocol cannot establish inter-rater consistency, implementation burden, supplier behavior, or the long-term relationship between commissioning evidence and operational outcomes.

Future research should validate ITCRAF in three stages. First, a multidisciplinary Delphi panel comprising utility, EPC, OEM, protection, automation, operations, cybersecurity, and safety experts should assess construct completeness, gate definitions, defect classifications, and proposed evidence. Second, pilot projects should measure inter-rater consistency, user effort, first-pass acceptance, defect-detection yield, energization delay, configuration deviations, early-life failures, misoperations, forced outages, and maintenance findings. Third, comparative or matched-project studies should test whether projects using ITCRAF differ from conventional projects after controlling for voltage level, architecture, contractor capability, and project complexity. Sensitivity

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

analysis should examine alternative CRI weights, readiness thresholds, scoring rules, and defect-classification rules. Additional technical studies should evaluate cybersecurity commissioning, digital-twin-assisted testing, process-bus interoperability, automated SCL validation, remote testing, and centralized protection-and-control architectures.

6. Conclusion

Modern substations are integrated cyber-physical systems whose reliability cannot be demonstrated through disconnected equipment tests. This paper developed ITCRAF, a five-gate lifecycle framework covering design assurance, factory acceptance, site acceptance, integrated commissioning and energization, and post-energization reliability assurance. The framework connects requirements, risks, tests, defects, configuration baselines, release decisions, and operational feedback.

The key contribution is the treatment of commissioning evidence as the first operational reliability baseline. Traceability shows why each test exists and what evidence it produces. Configuration control preserves the tested state. The CRI improves visibility of progress, while hard gates prevent unresolved safety or protection risks from being diluted by aggregate completion. The illustrative 132/33 kV scenario demonstrates how the approach can be applied without claiming empirical performance improvement.

For utilities and project organizations, the practical recommendation is to govern interfaces, evidence, and configuration baselines as rigorously as physical equipment. ITCRAF should be localized, independently reviewed, and piloted using the prospective case-study protocol defined in this paper before portfolio-wide adoption. The pilot should retain pre-consensus reviewer assessments and follow operational outcomes for at least 12 months, while subsequent matched-project research should test broader transferability and effectiveness. In Saudi Arabia, ITCRAF's strategic value is the creation of a consistent assurance chain across new substations and renewable

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

interconnections: approved requirements are linked to verified tests, critical defects block energization, tested configurations become operational baselines, and field events improve future projects. This governed learning cycle can support the reliable grid expansion, digital-network capability, and renewable-energy integration required by Vision 2030 while generating the empirical evidence needed for subsequent validation of the framework.

Acknowledgements

The author acknowledges the contribution of publicly available international standards summaries, official energy-sector sources, reliability guidance, and scholarly publications used in developing this technical framework.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Conflicts of Interest

The author declares no conflict of interest.

Ethical Approval

Not applicable. The study used publicly available documentary sources and an illustrative technical scenario. It did not involve human participants, animals, personal data, or confidential project records.

Data Availability

No new empirical dataset was generated or analyzed in this conceptual technical study. All documentary sources are identified in the reference list, and the illustrative scenario values,

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

framework components, analytical tables, and prospective case-study protocol required to understand and reproduce the proposed method are contained within the manuscript. Any dataset generated through future implementation of the protocol will require a separate data-management and availability statement consistent with applicable confidentiality, cybersecurity, contractual, and journal requirements.

Author Contributions

The author: Conceptualization; Methodology; Investigation; Formal analysis; Writing – original draft; Writing – review and editing.

Artificial Intelligence Use Disclosure

Generative artificial intelligence tools were used solely to support language refinement, structural organization, and document formatting. They were not treated as authors, evidence sources, or substitutes for technical judgment. The author reviewed and takes full responsibility for the technical content, originality, interpretation, accuracy of citations, and final submitted version.

Author Responsibility Statement

The author confirms substantial contributions to the conception, design, synthesis, analysis, interpretation, and writing of the manuscript. The author has reviewed and approved the final version and agrees to its submission for publication. As the corresponding author, Omer Sikander is responsible for ensuring the accuracy, integrity, and originality of the manuscript and for managing all correspondence relating to the submission.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

References

[1] International Energy Agency. Electricity Grids and Secure Energy Transitions. Paris: IEA; 2023. Available from: https://www.iea.org/reports/electricity-grids-and-secure-energy-transitions. Accessed 6 October 2026.

[2] International Electrotechnical Commission. IEC 61850: Communication networks and systems for power utility automation. IEC 61850 online resource. Available from: https://iec61850.dvl.iec.ch/. Accessed 6 October 2026.

[3] International Electrotechnical Commission. IEC 61850-5:2013+AMD1:2022 CSV: Communication networks and systems for power utility automation – Part 5: Communication requirements for functions and device models. Edition 2.1. Geneva: IEC; 2022. Available from: https://webstore.iec.ch/en/publication/75090. Accessed 15 October 2026.

[4] North American Electric Reliability Corporation. M-9 Protection System Misoperations. Atlanta: NERC. Available from: https://www.nerc.com/programs/reliability-assessment--performance-analysis/reliability-indicators/m-9-protection-system-misoperations. Accessed 6 October 2026.

[5] North American Electric Reliability Corporation. PRC-004-6: Protection System Misoperation Identification and Correction. Atlanta: NERC. Available from: https://www.nerc.com/globalassets/standards/reliability-standards/prc/prc-004-6.pdf. Accessed 6 October 2026.

[6] Ministry of Energy, Kingdom of Saudi Arabia. Electricity Sector Integration. Available from: https://www.moenergy.gov.sa/en/eco-system/programs/electricity-sector-integration/about. Accessed 6 October 2026.

[7] Ministry of Energy, Kingdom of Saudi Arabia. Renewable Energy. Available from: https://www.moenergy.gov.sa/en/eco-system/programs/renewable-energy. Accessed 6 October 2026.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

[8] Cowan A, Gray K, Colmenares E. Testing a Live Industrial Digital Substation with IEC 61850 Tools. Western Protective Relay Conference; 2024. Available from: https://wprcarchives.org/wp-content/uploads/2025/04/Aaron-Cowan_Testing-a-Live-Industrial-Digital-Substation-with-IEC-61850-Tools_2024.pdf. Accessed 6 October 2026.

[9] IEEE Standards Association. IEEE C37.300-2024: IEEE Guide for Centralized Protection and Control Systems within a Substation. New York: IEEE; 2024. Available from: https://standards.ieee.org/ieee/C37.300/7258/. Accessed 6 October 2026.

[10] Sutherland PE. Commissioning and Periodic Maintenance of Microprocessor Based Protection Relays in Industrial Facilities. IEEE PES and IAS Boston; 2022. Available from: https://site.ieee.org/boston-pes/files/2017/03/PeterSutherland_RelayTesting-Lecture-Boston4.26.22.pdf. Accessed 6 October 2026.

[11] Apostolov A. Efficient maintenance testing in digital substations based on IEC 61850 Edition 2. Protection and Control of Modern Power Systems. 2017;2:29. doi:10.1186/s41601-017-0054-0.

[12] Londoño Ospina J, Martinez del Sol A, Gaggero PA. Commissioning and start-up of digital substations under IEC 61850 standard. IET Conference Proceedings. 2025. doi:10.1049/icp.2025.1047.

[13] Mirhosseini M, Heydari A, Astiaso Garcia D, Mancini F, Keynia F. Reliability based maintenance programming by a new index for electrical distribution system components ranking. Optimization and Engineering. 2022;23:2315–2333. doi:10.1007/s11081-022-09767-8.

[14] Almutairi A, Alhamed Y. Sustainability and Grid Reliability of Renewable Energy Expansion Projects in Saudi Arabia by 2030. Sustainability. 2025;17(10):4493. doi:10.3390/su17104493.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

[15] International Energy Agency. Building the Future Transmission Grid. Paris: IEA; 2025. Available from: https://www.iea.org/reports/building-the-future-transmission-grid. Accessed 6 October 2026.

[16] International Electrotechnical Commission. IEC 61850-10:2012+AMD1:2025 CSV: Communication networks and systems for power utility automation – Part 10: Conformance testing. Edition 2.1. Geneva: IEC; 2025. Available from: https://webstore.iec.ch/en/publication/108858. Accessed 15 October 2026.

[17] International Electrotechnical Commission. IEC TR 61850-10-3:2022: Communication networks and systems for power utility automation – Part 10-3: Functional testing of IEC 61850 systems. Geneva: IEC; 2022. Available from: https://webstore.iec.ch/en/publication/61395. Accessed 15 October 2026.

[18] International Electrotechnical Commission and Institute of Electrical and Electronics Engineers. IEC/IEEE 61850-9-3:2016: Communication networks and systems for power utility automation – Part 9-3: Precision time protocol profile for power utility automation. Geneva/New York: IEC/IEEE; 2016. Accessed 15 October 2026.

[19] International Electrotechnical Commission. IEC 62351-6:2020: Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850. Geneva: IEC; 2020. Available from: https://webstore.iec.ch/en/publication/63742. Accessed 15 October 2026.

[20] North American Electric Reliability Corporation. PRC-005-6: Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance. Atlanta: NERC. Available from: https://www.nerc.com/globalassets/standards/reliability-standards/prc/prc-005-6.pdf. Accessed 15 October 2026.

[21] International Organization for Standardization. ISO 55001:2024: Asset management – Asset management system – Requirements. 2nd ed. Geneva: ISO; 2024. Available from: https://www.iso.org/standard/83054.html. Accessed 15 October 2026.

CC BY

Nexus Science Review
INTERNATIONAL JOURNAL OF INTERDISCIPLINARY RESEARCH

Received: 15/09/2026 - **Accepted:** 17/10/2026
Vol: 01.05
DOI: 10.66104/zz710039
Pages: 1-31

[22] National Grid SA. Saudi Arabian Grid Code. Version May 2026. Approved by the Saudi Electricity Regulatory Authority. Riyadh; 2026. Available from: https://www.se.com.sa/-/media/sec/About-Us/National-Grid-SA/Saudi-Arabian-Grid-Code-Guide/English/SAGC-Grid-Code-May-2026.ashx. Accessed 15 October 2026.

[23] National Cybersecurity Authority, Kingdom of Saudi Arabia. Operational Technology Cybersecurity Controls (OTCC-1:2022). Riyadh: NCA; 2022. Available from: https://nca.gov.sa/en/regulatory-documents/controls-list/otcc/. Accessed 15 October 2026.

[24] International Electrotechnical Commission. IEC 60255-1:2022: Measuring relays and protection equipment – Part 1: Common requirements. 2nd ed. Geneva: IEC; 2022. Available from: https://webstore.iec.ch/en/publication/59762. Accessed 15 October 2026.

CC BY