Building Scalable and Interoperable Digital Collaboration Ecosystems for Saudi Vision 2030: Integrating Enterprise Video Conferencing, Voice Communications, and Hybrid Cloud Infrastructure.

Abstract

Saudi Vision 2030 demands digital services that connect institutions, specialists and citizens without creating brittle dependencies on individual communication platforms. This critical review examines how enterprise video conferencing, Internet Protocol voice and hybrid cloud infrastructure can form a scalable, interoperable collaboration ecosystem, with particular attention to the electrical systems that sustain digital operations. A structured synthesis of 2020–2025 research evaluates media quality, federated identity, open interfaces, edge orchestration, cyber resilience and energy continuity. The proposed framework separates user experience, communication signalling, media processing, identity governance and underlying power dependencies, while establishing explicit boundaries between enterprise collaboration and operational technology. Evidence supports hybrid deployments as a conditional architectural choice rather than a universal optimisation: local survivability and data control must be weighed against operational complexity, integration risk and duplicated capacity. Two analytical matrices identify interoperability constraints and assurance priorities. The review contributes an implementable reference architecture, risk-informed migration sequence and falsifiable evaluation criteria for Saudi public institutions, financial enterprises and electricity-dependent services. It concludes that measurable user experience, standards-based portability, segmented trust and tested power-continuity arrangements are more defensible indicators of transformation than platform adoption alone.

Keywords: *Unified communications; enterprise videoconferencing; voice over IP; hybrid cloud; interoperability; Saudi Vision 2030; electrical resilience; cybersecurity*

1. Introduction

Enterprise collaboration has moved from a discrete communications function to a dependency of organisational continuity. Hybrid work, distributed project delivery and digital public services require speech, video, messaging and content sharing to cross physical locations and administrative domains. Yet integration is not achieved by placing these functions in one procurement package. Telemeeting research establishes that quality of experience includes conversational dynamics, task suitability and psychological factors alongside network performance [1]. Work on time-varying video quality also shows why aggregate throughput

UNDER PEER REVIEW IN IJAR

cannot explain perceived service quality [2]. These findings challenge a technology-led definition of collaboration maturity: connecting endpoints is necessary, but the relevant outcome is whether people can coordinate decisions accurately and securely.

For Saudi Arabia, the challenge is structurally distinctive. Vision 2030 encourages digitally enabled public administration, advanced industry and geographically dispersed economic projects. Collaboration must extend between metropolitan headquarters, regional facilities, suppliers and mobile professionals. A mobile field engineer may require a reliable voice escalation and shared visual diagnosis while a central operations centre coordinates several organisations. Real-world WebRTC measurements show that radio conditions, handover and operator choice materially affect communication quality [3]. Therefore, nominal fifth-generation coverage cannot be substituted for end-to-end assurance. The architecture must also recognise unequal endpoint capability, intermittent connections and the different confidentiality expectations associated with ordinary meetings, financial discussions and infrastructure incidents.

Human factors make further requirements unavoidable. Bennett and colleagues associate videoconference experiences with fatigue and social belonging, while the Zoom Exhaustion and Fatigue Scale establishes a multidimensional way to investigate adverse experiences [4,5]. Consequently, an ecosystem cannot be declared sustainable solely because meeting capacity has increased. Excessive mandatory video use, poor accessibility, fragmented calendars and authentication friction can reduce participation despite technically successful sessions. At the institutional level, the cost of proprietary connectors, duplicated identity stores and incompatible recording formats may lock agencies into one supplier. At the physical level, uninterrupted communications rely upon electricity, cooling and functioning network premises. A credible Saudi collaboration strategy must address all three dimensions together: user value, inter-organisational technical compatibility and infrastructure survivability.

2. Aim, research questions and contribution

The aim is to develop and critically assess a reference architecture for scalable, interoperable enterprise collaboration in Saudi Arabia, incorporating voice, video, hybrid cloud and electrical resilience. Four objectives guide the synthesis: identify open interoperability boundaries; compare centralised, local and distributed media placement; design identity, security and continuity controls across trust domains; and establish measurable operational acceptance criteria. The review asks which functions should remain local, which can be federated, how failure should be contained and what evidence would justify each deployment choice. Its contribution is conceptual and design-oriented, not a claim of experimentally demonstrated superiority. The figures represent

UNDER PEER REVIEW IN IJAR

proposed mechanisms, whereas the tables contain reasoned qualitative assessments that require field validation.

3. Review methodology and evidential boundaries

A structured critical narrative review was developed from scholarly articles, research repositories, standards publications and publisher records issued between 2020 and 2025. Searches combined terms such as “videoconferencing quality of experience”, “WebRTC mobile quality”, “cloud-edge orchestration”, “intercloud federation”, “zero trust cloud”, “Saudi smart grid security” and “data centre power systems”. Material was included when it provided a relevant empirical study, technical model, review, or standards-based architectural argument with identifiable bibliographic metadata and a DOI. The resulting corpus deliberately spans communications engineering, information systems, human factors, cybersecurity and energy research. Studies devoted exclusively to consumer entertainment or to electrical protection algorithms without collaboration relevance were not treated as primary architectural evidence.

For transparency, this is neither a census of all indexed publications nor a statistical meta-analysis. The searches were purposive, the thirty selected sources are heterogeneous and no reproducible database-wide screening count is asserted. Assessment therefore prioritised mechanisms, assumptions, methodological limitations and transferability rather than pooled effect sizes. A controlled vocabulary was used to distinguish signalling, media, control planes, identity, cloud portability and power availability. Findings were compared through four lenses: interoperability, performance, security and operational sustainability. Conflicting evidence was retained; for example, the latency advantages of edge deployment were compared against distributed management overhead, and claimed energy savings were checked against the boundaries used to calculate them.

Strength of inference varies by source. Measurement studies of videoconferences and mobile networks provide more direct evidence for user experience than surveys of general edge-computing systems. Conversely, Saudi smart-grid publications illuminate local power-sector constraints but do not establish performance benefits for enterprise calling. The review uses these latter studies to define dependencies and governance boundaries, not to infer call-quality gains. Architectural implications are explicitly framed as hypotheses for procurement trials, pilot measurement and resilience exercises. This distinction avoids portraying cross-domain extrapolation as validated deployment evidence and explains why the proposed indicators favour transparent baselines, paired tests and auditable failure scenarios.

Appraisal distinguished direct observation, prototypes, reviews and conceptual proposals. For each source, we recorded system boundaries, workloads, proprietary dependencies, outcomes and

UNDER PEER REVIEW IN IJAR

validity constraints. Comparisons were considered stronger when metrics were collected under explicitly described network or power conditions, and weaker when only theoretical capability or provider features were reported. No numerical weighting was assigned across dissimilar disciplines: the ethical implications of recording access, for example, cannot meaningfully be averaged with measured packet delay. This approach also protects the analysis against double counting claims repeated by several surveys without independent experiments.

4. Architectural foundations: from endpoints to hybrid control

A digital collaboration ecosystem has at least five logically separable components: user endpoints, session signalling, real-time media paths, application integrations and shared governance. Standards-based clients support device diversity, but successful negotiation also depends on codec overlap, network traversal and the trust model of each participating organisation. A video session may establish through cloud-hosted signalling while its media follows a regional relay, a local bridge or a direct encrypted path. Voice introduces further dependencies through dial plans, emergency routing, legacy private branch exchanges, call admission and public telephone interconnection. Treating these functions as a single indivisible platform obscures where faults occur and which components may be migrated independently.

Figure 1 formalises a hybrid topology in which enterprise sites and mobile users connect to a policy-controlled collaboration plane. Local session border controllers and survivable calling functions remain available for appropriately selected service groups, while cloud services provide elastic conferencing, directory federation and administration. Media services are placed through explicit policies rather than assuming that every packet should cross a central data centre. Evidence on multi-access edge video delivery indicates potential reductions in transport burden, but demonstrates that caching, compute placement and resource allocation require careful orchestration [6]. Broad surveys of multi-access edge computing likewise describe constrained resources and service-specific trade-offs [7]. Accordingly, local media processing should be triggered by tested latency, regulation or outage requirements, not by architectural fashion.

Scalability should be defined along independent axes. Horizontal media scale concerns conference concurrency and transcoding demands; signalling scale concerns registration, session establishment and failover; administrative scale concerns tenant boundaries, provisioning and troubleshooting. Chiang and colleagues demonstrate the complexity of orchestration across heterogeneous edge resources [8], while Costa and co-authors identify overlapping but distinct fog orchestration and resource-management responsibilities [9]. These observations make a single global autoscaling policy implausible. An adaptive design needs regional resource pools,

UNDER PEER REVIEW IN IJAR

topology-aware placement, admission protection and reserved headroom for incident surges. It must also detect when a smaller local cluster has become an operational single point of failure.

Hybrid infrastructure creates coordination costs. Federated cloud-edge-fog research shows how offloading decisions depend jointly on latency, compute capacity, connectivity and uncertain workload information [10]. In practice, every additional location introduces certificate lifecycles, telemetry pipelines, change windows and vendor support relationships. The appropriate balance is therefore a modest number of well-governed failure domains rather than indiscriminate distribution. Figure 1 separates critical trust functions from elastic media capacity and marks the electrical-support layer beneath both. No arrow implies unrestricted network access: every inter-zone crossing is subject to authorisation, routing policy and logging.

Multi-access edge computing research identifies the attraction of proximity but also exposes the complexity of mobility management and workload placement [11]. Regional routing decisions should follow observed paths rather than administrative geography. A private breakout at a remote site may improve local voice continuity, while a cloud bridge may better support unusually large inter-agency events. Selecting either path requires advance knowledge of endpoint capabilities, carrier reachability and local compute capacity. Crucially, the control plane must not make an unavailable remote directory a prerequisite for every locally recoverable call, although exceptional continuity modes still require logged and time-limited permissions.

REVIEW IN IJAR

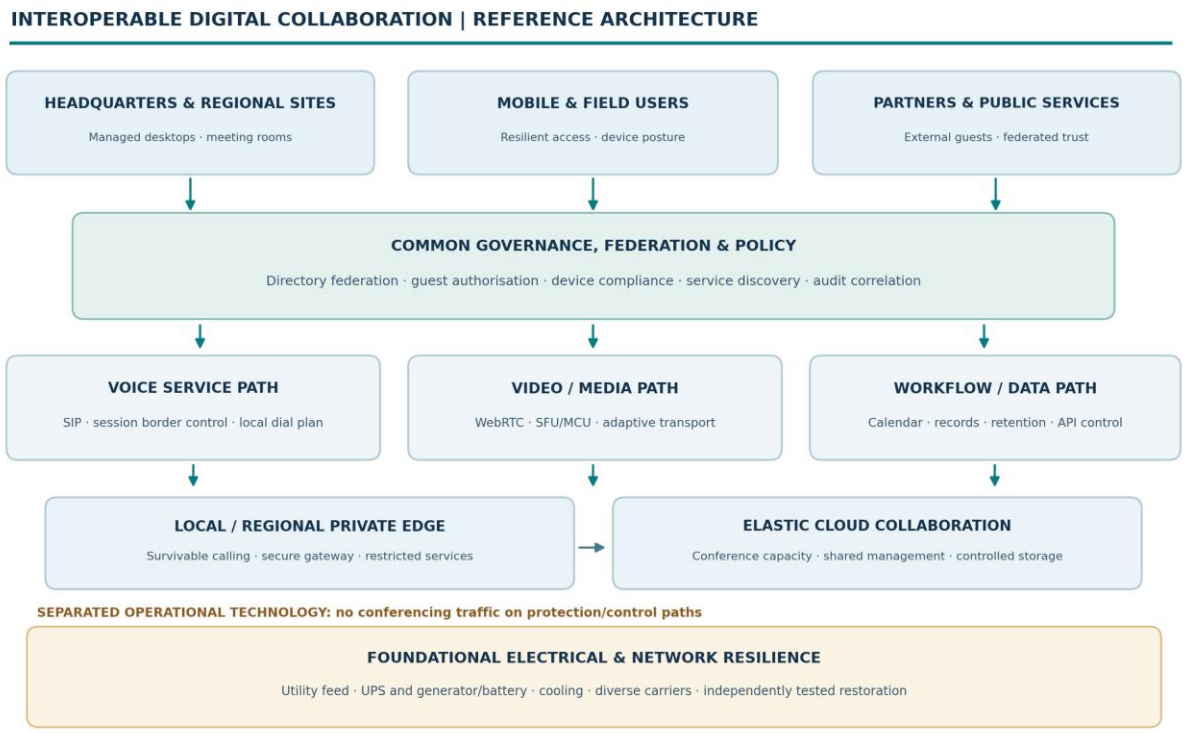


Figure 1. *Proposed layered architecture integrating enterprise voice, conferencing, federated governance, hybrid delivery and electrical resilience. Original conceptual synthesis; arrows denote governed service relationships, not unrestricted trust.*

5. Interoperability and portability as measurable properties

Interoperability must be tested at protocol, semantic and organisational levels. Protocol compatibility covers session establishment, media negotiation, transport security and directory interfaces. Semantic compatibility covers meeting identifiers, participant roles, retention labels, device states and emergency-call behaviour. Organisational compatibility determines whether two parties recognise each other's identities, permissions and incident responsibilities. Bohn and Lee describe intercloud federation as a standards-based route to sharing resources between distinct providers [12], and Bohn positions application programming interfaces as enabling mechanisms for practical federation [13]. Neither source implies that cloud federation automatically produces end-to-end voice or video interworking. Collaboration-specific conformance testing remains indispensable.

Table 1 translates these layers into observable tests. For voice, gateways must demonstrate correct caller identity, dial plan translation, encrypted signalling where applicable, codec negotiation and service continuity after a wide-area failure. For video, test participants should join across heterogeneous clients while recording whether participant admission, content sharing, captions, layouts and encryption remain consistent. Directory integration must preserve joiner, mover and leaver states without exposing privileged accounts to uncontrolled synchronisation. Calendar and recording connectors require exportable metadata, retention enforcement and revocation. A connector that works only when a proprietary account holds administrative rights is an integration liability, not evidence of open portability.

The principal design tension is that interoperability can increase the attack surface. Every gateway translates security assumptions as well as message formats; transcoding can terminate media encryption; and federation can redistribute personal information beyond the originating institution. The answer is not to prohibit integration but to document where trust terminates, which data are replicated and whether an alternative provider could replace a component without rebuilding identities and workflows. Middleware research demonstrates the value of abstraction for reducing cloud portability work, while acknowledging latency overhead [14]. A defensible procurement test should therefore require reproducible export, staged migration and independently witnessed interoperability exercises before considering a product interchangeable.

A further distinction concerns compatibility at installation and compatibility throughout service evolution. A connector that passes a pilot can fail after changes to authentication claims,

UNDER PEER REVIEW IN IJAR

supported codecs or application programming interfaces. Contractual portability should consequently require a published interface inventory, version-support windows, regression-test fixtures and a defined remediation path when an interface changes. Saudi organisations contracting across several providers also need synchronisation and correlation identifiers to trace one incident through identity, signalling, media and recording components. Without such shared evidence, incident ownership becomes disputed, restoration is delayed and apparent federation remains an administrative arrangement rather than an operational capability.

Table 1. *Interoperability acceptance matrix: cross-provider compatibility and auditable deployment criteria.*

Interface / layer	Failure mechanism	Acceptance evidence	Saudi deployment relevance
Voice signalling and PSTN	Identity or number translation fails; media routed through incorrect trunk	Two providers complete inbound/outbound and priority calls; verify security, failover and dial plan	Regional sites require documented carrier diversity and local survivable calling
Cross-platform meetings	Negotiation succeeds but share, captions or guest roles disappear	Repeat meeting test across heterogeneous endpoints; capture feature-level pass/fail evidence	Inter-agency services need accessible external participation
Identity and directories	Federated roles or revocation drift between systems	Test joiner/mover/leaver workflow, conditional access, guest expiry and audit trace	Contractor-heavy projects need controlled temporary access
Records and workflow APIs	Transcript retention, deletion or export semantics differ	Export and re-import metadata; verify access restrictions and deletion consistency	Apply institutional classification and approved retention requirements
Hybrid-cloud management	Provider change disrupts monitoring or resource placement	Demonstrate configuration rollback, portable logs and multi-domain recovery	Manage site, carrier and electrical dependencies as explicit failure domains

6. Voice, conferencing and quality of experience

Voice and video share packet transport but have different failure sensitivities. Speech is acutely affected by jitter, clipping, echo and conversational delay; video adds visual artefacts, frame instability, lip synchronisation and screen-content legibility. Operators should monitor distributions of end-to-end latency, packet loss and jitter together with media concealment and user-reported experience. Averages can conceal short bursts that destroy intelligibility. The synthesis of Skowronek and colleagues [1] and Hewage and colleagues [2] favours multimodal assessment rather than equating network quality of service with perceived quality of experience. Indicators should be segmented by site, access medium, endpoint category and meeting type, with consent-aware sampling and clear data minimisation.

For Internet telephony, session initiation, routing and media continuity must be distinguished in incident diagnosis. A successful session setup does not prove that downstream media will survive a route change. Session border controllers should enforce topology hiding, rate limits, protocol validation and transparent handling of emergency or regulated calls. Research on Session Initiation Protocol caller-identity abuse illustrates how signalling weaknesses can undermine voice trust even when audio remains available [15]. Encrypted media and strong authentication are important, but they cannot independently prevent toll fraud, account misuse or denial of service. Inbound carrier diversity and local fallback must be tested with the same seriousness as conference scaling.

For video, selective forwarding conserves processing by forwarding suitable streams, whereas multipoint mixing can simplify older endpoint interoperability at greater compute cost and reduced end-to-end confidentiality. Edge transcoding may improve access from constrained networks but creates extra keys, recording controls and power demands. WebRTC quality research shows that mobile handovers and changing radio conditions complicate consistent service levels [3]. Hence congestion control should protect speech before optional high-resolution video, and shared presentations should adapt without destroying readable text. Network slicing and transport orchestration offer mechanisms for service differentiation, yet Manso and colleagues show that multi-domain execution requires coordinated management [16], while Afolabi and colleagues emphasise distributed slice configuration [17]. Such approaches are options for controlled networks, not guaranteed remedies for Internet paths.

User-centred policy is part of engineering. Bennett and colleagues [4] associate fatigue with meeting conditions, while later work frames videoconferencing fatigue as an organisational labour issue rather than solely an interface defect [18]. A design that mandates continuous cameras or complex tool switching can reduce value even when packet metrics improve. Enterprises should

UNDER PEER REVIEW IN IJAR

permit audio-first participation, clear meeting purposes, accessible captions and alternative asynchronous channels. Behavioural evidence supports such governance, but does not establish one universal threshold for appropriate video use. Evaluation must therefore combine network measurements, task completion and participant feedback, with the latter interpreted carefully to avoid treating self-report as a direct measure of infrastructure reliability.

7. Identity, cybersecurity and cross-domain trust

The hybrid collaboration perimeter is porous by construction: external guests, contractors, cloud services and legacy voice trunks all interact with internal identities. A zero-trust approach is consequently preferable to network-location assumptions. Ferretti and colleagues demonstrate the importance of survivability even when security control components are attacked [19]. A service that authenticates every request but loses its sole policy engine during an outage may be secure on paper and unavailable in practice. Identity-provider redundancy, scoped tokens, device posture, privileged-access separation and recovery procedures should be treated as mutually dependent controls rather than independent product features.

Cloud security reviews identify layered threats across infrastructure, platforms and software [20], while newer hybrid-cloud work highlights privacy, regulatory and provider-heterogeneity tensions [21]. This justifies fine-grained separation of data, control and media planes. Identity federation can use established open mechanisms, but the mapping of roles, lifecycle states and conditional-access policies must be documented. Management APIs require narrow scopes, workload identity and rotation. Call recordings, transcripts and metadata deserve dedicated classification because participant names and discussion topics can remain sensitive even when media content is encrypted. Retention periods, lawful access and residency assessments must be established by relevant Saudi institutional authorities rather than inferred from a supplier’s marketing claims.

A useful boundary concerns operational technology. Electricity control networks, protection relays and substation automation have different availability and determinism requirements from meeting platforms. Their protection traffic should never be routed through a corporate conferencing service, even if an integration demonstration appears convenient. Any operational collaboration bridge should export carefully filtered incident information into a separated environment, with unidirectional or tightly mediated flows where warranted. Research focused on Saudi smart-grid information security emphasises risks associated with bidirectional data exchange [22]. Its relevance here is architectural isolation and cyber governance, not permission to merge operational and enterprise networks. Vendor remote support should use temporary access approvals, monitored sessions and explicit expiry.

UNDER PEER REVIEW IN IJAR

Cross-domain collaboration requires a distinction between authenticating a known device and authorising a particular activity. A contractor may need temporary participation in a maintenance meeting without permission to search historical recordings, inspect the enterprise directory or administer a gateway. Policies should separately govern invitation validity, document transmission, transcription, retention and external sharing. Emergency procedures must also distinguish reduced convenience from unsafe privilege escalation: temporary local calling can be legitimate during federation failure, whereas unrestricted access to sensitive collaboration archives is not. Research on cybersecurity during energy-sector digital transformation reinforces the need to align organisational controls with changing operational exposure [23].

8. Electrical infrastructure, energy and Saudi context

Physical continuity is the least visible dependency in cloud collaboration diagrams. Local routers, radio equipment, session gateways, server rooms, switching fabrics and cooling all require dependable electrical supply. A regional conference service may be geographically redundant while both enterprise access circuits terminate in a building with one distribution board. Accordingly, a complete resilience model must trace utility feed, automatic transfer, uninterruptible power supply, generator or battery endurance, cooling, and diverse network routes. Capacity planning should distinguish the energy needed for brief ride-through from that required for sustained operations, and verify maintenance arrangements under realistic thermal and peak-load conditions.

Saudi smart-grid research describes the interaction of digital communications, renewable integration and secure information flows [24]. A digital-twin study likewise explores potential links among grid monitoring, sustainability and security, while its prototype context limits straightforward generalisation to nationwide infrastructure [25]. These studies suggest two implications for collaboration design. First, an enterprise can strengthen electricity-sector coordination through secure incident conferencing without placing control traffic on meeting infrastructure. Second, the enterprise collaboration estate must itself tolerate supply disturbance during grid modernisation and renewable penetration. Neither implication establishes a measured causal effect of collaboration technology on electricity reliability; that relationship requires operational evaluation.

Energy accounting also needs methodological discipline. Research on data-centre electrical supply systems emphasises efficiency, storage and renewable integration [26]. Mytton and colleagues caution that network electricity use does not increase linearly with transmitted data [27], undermining simple claims that reducing video bitrate saves a proportional quantity of power. Grid-oriented research on flexible data-centre demand suggests the possibility of shifting

UNDER PEER REVIEW IN IJAR

computational loads under particular operating assumptions [28]. For Saudi procurement, this argues for workload-level energy measurements, transparent power-usage-effectiveness boundaries and resilient renewable sourcing rather than a generic “green cloud” label. Local transcoding could reduce external transport but increase server cooling, while cloud consolidation might lower on-premises equipment demand yet raise sovereignty or outage exposure.

Saudi Vision 2030 also has an institutional dimension. Research on the country's transition from electronic government to digital government identifies technology adequacy and organisational change as complementary enablers [29]. Thus an electricity-backed communications ecosystem must be governed across information technology, facilities, security, procurement and business continuity teams. Sector-specific exercises should involve simulated building power loss, carrier disruption and identity-service failure with real users. The outcome should be recorded in actual call restoration, meeting reconnection and incident decision times, not only in the availability claims of contracted cloud regions.

Availability modelling should expose shared electrical failure modes rather than merely count nominally independent servers. Two conference nodes connected to different switches can still depend on one power distribution unit, one cooling circuit or one telecommunications room. Acceptance testing therefore needs an end-to-end dependency map connecting each designated critical call path to facility supply, switching, carrier access and identity services. During a generator transfer exercise, assess not just whether equipment remains powered, but whether voice registration survives, media paths recover and staff can convene an incident call. Test plans must protect operational equipment and use authorised simulation rather than disruptive experiments on live electrical controls.

UNDER PEER REVIEW IN IJAR

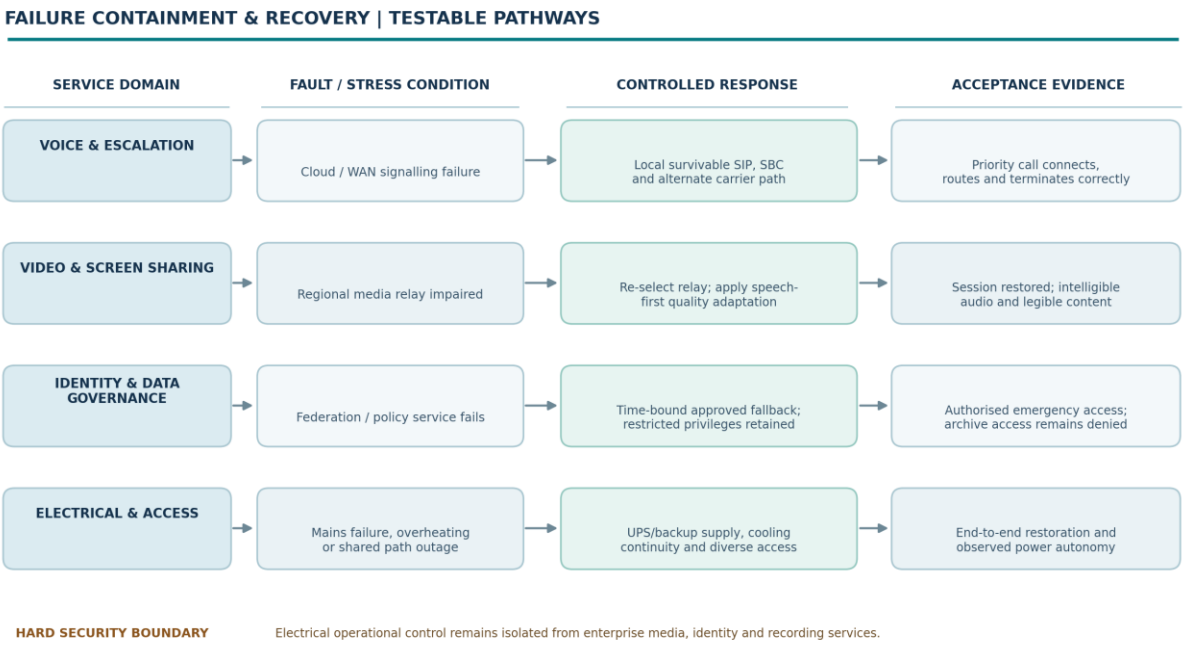


Figure 2. *Original failure-containment pathways for voice, conferencing, identity and electrical supply. Each response is linked to an observable acceptance test; operational control traffic remains isolated.*

9. Evaluation framework and staged adoption

Table 2 proposes a verification matrix without manufacturing benchmark results. An implementation should establish a baseline at representative Saudi locations, including headquarters, regional offices and critical facilities. Measurements should sample busy hours, mobile handovers, restricted guest networks and degraded power states. Quality thresholds must be approved for each service class; importing a single global latency or uptime target risks disguising differences between routine training, financial authorisation meetings and emergency coordination. Successful interoperability is demonstrated by pre-declared pass criteria across different devices and providers, not by one prepared demonstration. Security acceptance similarly requires evidence of revocation, restricted recording access, administrative failover and audit-log integrity.

A migration can proceed in four controlled phases. First, discover call flows, integrations, electrical dependencies and data classes, then document actual failure domains. Second, introduce identity federation and limited pilot interoperability, retaining stable local voice routes. Third, migrate selected conferencing workloads into elastic regional pools while validating guest access, recording governance and observability. Fourth, test survivable voice, alternative carriers, identity outages and power loss before reducing redundant legacy components. Distributed management

UNDER PEER REVIEW

research warns that network controllers can themselves become coordination dependencies [8,10]; migration gates should therefore require rollback procedures, configuration snapshots and independently verified recovery. An operating model should assign one accountable owner for each cross-provider incident.

The architecture should be evaluated against alternatives rather than presumed optimal. A fully centralised cloud approach can simplify operations but may fail under external connectivity loss. An entirely local estate can improve direct control yet make multi-party capacity and software maintenance expensive. A hybrid design can combine benefits while multiplying integration surfaces and coordination burdens. Evidence from cloud federation [12,13] and emerging network slicing [17] supports the feasibility of controlled interconnection, not the proposition that hybrid architecture always reduces lifetime cost. Decisions must incorporate recurring licence expenditure, specialist staffing, power plant maintenance, audit effort and the probability and impact of service disruption.

An assurance scorecard should distinguish service availability, recoverability and fitness for purpose. Availability describes whether an endpoint can reach a function; recoverability records restoration time and data loss following a declared fault; fitness assesses speech intelligibility, caption reliability, screen readability and successful completion of the intended task. Measurements require paired baseline and intervention periods, site-level stratification and documented exception handling. Results should include the distribution of poor sessions, not only central tendencies. Cost evaluation similarly needs a common functional unit, such as a completed supported meeting or a successfully routed incident escalation, while explicitly recording the electricity, staffing and licensing assumptions behind each comparison.

Table 2. *Risk-weighted architectural alternatives and tests for representative Saudi collaboration use cases.*

Use case / stress	Preferred design hypothesis	Expected advantage	Principal exposure	Evidence needed
Routine multi-agency meeting	Federated cloud conference with controlled guest access	Elastic capacity and cross-site reach	Recording leakage; role mismatch; vendor lock-in	Join, share, caption, revoke and export across platforms

UNDER PEER REVIEW IN IJAR

Use case / stress	Preferred design hypothesis	Expected advantage	Principal exposure	Evidence needed
Utility field escalation	Audio-first hybrid session with local call route	Speech continuity under changing radio conditions	Carrier failure; accidental operational-network bridging	Handover test and filtered incident-data flow
Remote-site WAN outage	Local SIP survivability and approved alternate trunk	Retains necessary voice escalation	Local hardware, trunk and power common-mode failures	Timed priority-call exercise after cloud isolation
Compromised identity / policy	Segmented federation and least-privilege fallback	Contains lateral access without losing essential calls	Emergency bypass of sensitive records	Revocation and deny-by-default tests during service failure
Facility electrical disturbance	Resilient network room and diverse powered paths	Maintains service through supply transfer	Shared cooling, switchboard or carrier termination	UPS autonomy, failover and end-to-end restoration drill

10. Critical discussion and limitations

The central finding of this synthesis is conditional: interoperability and resilience improve only when the system exposes boundaries that can be verified independently. Open signalling without shared semantics leaves inconsistent caller identities; cloud federation without exit testing creates hidden lock-in; duplicated media capacity without independent power and identity dependencies offers weak redundancy. These are architectural inferences from complementary studies, not pooled experimental findings. The strongest evidence concerns narrower mechanisms such as mobile quality variation, edge resource trade-offs, cloud security hazards and data-centre electricity systems. Few studies evaluate all of these within one Saudi enterprise collaboration deployment.

Several limitations constrain generalisation. The reviewed studies use different performance metrics, workloads, geographies and methodological designs. Mobile network observations cannot be applied unchanged to fixed campus networks, while electricity-sector cybersecurity findings do not quantify collaboration availability. Proprietary conferencing implementations may

UNDER PEER

restrict inspection of media routing, algorithmic adaptation and identity interfaces. The review offers no Saudi field trial, comparative cost dataset, penetration-test outcome or quantified carbon reduction. Its tables are qualitative analytical tools, not measured scores. Researchers and procurement teams should regard the framework as a specification for falsifiable testing rather than a certified design or regulatory determination.

A recurring weakness in technology advocacy is the conflation of component resilience with organisational resilience. An independently redundant bridge has limited value if users cannot discover the fallback route, if guest permissions expire during an incident, or if the emergency call tree assumes a functioning corporate directory. Human procedures, change management and periodic drills are therefore part of the effective system boundary. Moreover, vendor-neutral standards do not remove supplier concentration in operational expertise, service contracts or data extraction tooling. These structural dependencies can dominate migration costs even where technical protocol compliance is demonstrated, and they should be disclosed in investment appraisals.

11. Research gaps and future directions

Four research gaps merit priority. First, there is insufficient cross-provider evidence on complete meeting interoperability, including captions, content sharing, recordings and role preservation, rather than merely successful connections. Second, mobile and fixed user experience should be studied jointly with task outcomes, accessibility and meeting fatigue, following insights from technostress research [30]. Third, the interaction between regional media placement and electrical continuity requires paired measurement of network conditions, power faults, cooling demands and recovery behaviour. Fourth, security studies should measure how identity-provider compromise or unavailable policy services affect emergency collaboration without relaxing authorisation controls.

Future studies should use reproducible multi-site pilots and pre-register service classes, outage scenarios and metrics. Controlled comparisons could evaluate local, cloud and hybrid placements under matched workloads; longitudinal work could examine inclusion, staff burden and operational cost. Electrical-sector trials should keep protection and control functions isolated while testing whether secure collaboration improves human incident response. Interoperability conformance suites, auditable data-export procedures and lifecycle energy inventories would make procurement claims more testable. Such research would establish whether the proposed architecture creates measurable public value rather than merely combining familiar technologies in one diagram.

UNDER PEER REVIEW IN IJAR

A useful research design would compare several Saudi site classes using identical scripted conversations, fault injections and recovery criteria. Rural field facilities, dense urban campuses and restricted industrial premises would reveal different bottlenecks. Report endpoint, access-network and computing energy, and only genuinely displaced travel. A parallel qualitative study could test whether better connectivity actually reduces decision delay or simply increases meeting frequency. Publishing negative results, interoperability failures and confidence intervals would materially improve the evidence base for future infrastructure procurement.

12. Conclusion

Scalable digital collaboration for Saudi Vision 2030 requires more than conferencing capacity. The viable design is a governed combination of interoperable endpoints, explicit media and signalling boundaries, federated identity, locally survivable voice, elastic hybrid services and verifiable electrical continuity. Research supports individual design mechanisms but not a universal claim that hybrid deployment outperforms alternatives. Saudi institutions should therefore evaluate cross-provider functionality, user experience, cyber isolation, energy use and outage recovery through representative trials. Most importantly, corporate collaboration must support electricity-sector coordination without becoming part of safety-critical control paths. Standards-based exit options, accountable operations and measurable resilience turn digital adoption into a defensible transformation programme.

References

[1] Skowronek, J.; Raake, A.; Berndtsson, G.H.; et al. (2022). Quality of Experience in Telemeetings and Videoconferencing: A Comprehensive Survey. *IEEE Access*, 10, 63885–63931. https://doi.org/10.1109/ACCESS.2022.3176369

[2] Hewage, C.T.E.R.; Ahmad, A.; Mallikarachchi, T.; Barman, N.; Martini, M.G. (2022). Measuring, Modeling and Integrating Time-Varying Video Quality in End-to-End Multimedia Service Delivery: A Review and Open Challenges. *IEEE Access*, 10, 60267–60293. https://doi.org/10.1109/ACCESS.2022.3180491

[3] Nakazato, J.; Nakagawa, K.; Itoh, K.; et al. (2024). WebRTC over 5 G: A Study of Remote Collaboration QoS in Mobile Environment. *Journal of Network and Systems Management*, 32, article 1. https://doi.org/10.1007/s10922-023-09778-5

[4] Bennett, A.A.; Campion, E.D.; Keeler, K.R.; Keener, S.K. (2021). Videoconference fatigue? Exploring changes in fatigue after videoconference meetings during COVID-19. *Journal of Applied Psychology*, 106, 330–344. https://doi.org/10.1037/apl0000906

UNDER PEER REVIEW IN IJAR

[5] Fauville, G.; Luo, M.; et al. (2021). Zoom Exhaustion & Fatigue Scale. *Computers in Human Behavior Reports*, 4, 100119. https://doi.org/10.1016/j.chbr.2021.100119

[6] Jiang, X.; Yu, F.R.; Song, T.; Leung, V.C.M. (2021). A Survey on Multi-Access Edge Computing Applied to Video Streaming: Some Research Issues and Challenges. *IEEE Communications Surveys & Tutorials*, 23, 871–903. https://doi.org/10.1109/COMST.2021.3065237

[7] Filali, A.; Abouaomar, A.; Cherkaoui, S.; Kobbane, A.; Guizani, M. (2020). Multi-Access Edge Computing: A Survey. *IEEE Access*, 8. https://doi.org/10.1109/ACCESS.2020.3034136

[8] Chiang, Y.; Zhang, Y.; Luo, H.; et al. (2023). Management and Orchestration of Edge Computing for IoT: A Comprehensive Survey. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2023.3245611

[9] Costa, B.G.S.; Bachiega Junior, J.; Carvalho, L.R.; Araújo, A.P.F. (2023). Orchestration in Fog Computing: A Comprehensive Survey. *ACM Computing Surveys*, 55(2), article 29, 1–34. https://doi.org/10.1145/3486221

[10] Kar, B.; Yahya, W.; Lin, Y.D.; Ali, A. (2023). Offloading Using Traditional Optimization and Machine Learning in Federated Cloud–Edge–Fog Systems: A Survey. *IEEE Communications Surveys & Tutorials*. https://doi.org/10.1109/COMST.2023.3239579

[11] Pham, Q.-V.; et al. (2020). A Survey of Multi-Access Edge Computing in 5G and Beyond: Fundamentals, Technology Integration, and State-of-the-Art. *IEEE Access*, 8, 116974–117017. https://doi.org/10.1109/ACCESS.2020.3001277

[12] Bohn, R.B.; Lee, C. (2022). The IEEE 2302-2021 Standard on Intercloud Interoperability and Federation. *IEEE Cloud Continuum*, 2(1). https://doi.org/10.1109/IEEESTD.2022.9732072

[13] Bohn, R.B. (2022). The Path to Cloud Federation through Standardization. *Proceedings of the International Conference on Information and Communication Technology Convergence*. https://doi.org/10.1109/ICTC55196.2022.9952660

[14] Bharany, S.; Kaur, K.; Badotra, S.; et al. (2022). Efficient Middleware for the Portability of PaaS Services Consuming Applications among Heterogeneous Clouds. *Sensors*, 22, 5013. https://doi.org/10.3390/s22135013

[15] Lema, H.; et al. (2023). Security Enhancement of SIP Protocol in VoIP Communication. *Journal of ICT Systems*, 1, 71–92. https://doi.org/10.56279/jicts.v1i2.32

[16] Manso, C.; Alemany, P.; Vilalta, R.; Muñoz, R.; Casellas, R.; Martínez, R. (2021). End-to-End SDN/NFV Orchestration of Multi-Domain Transport Networks and Distributed

UNDER PEER REVIEW IN IJAP

Computing Infrastructure for Beyond-5G Services. *IEICE Transactions on Communications*, E104-B, 188–198. https://doi.org/10.1587/transcom.2020NVI0001

[17] Afolabi, I.; Bagaa, M.; Boumezer, W.; Taleb, T. (2021). Toward a Real Deployment of Network Services Orchestration and Configuration Convergence Framework for 5G Network Slices. *IEEE Network*, 35, 242–250. https://doi.org/10.1109/MNET.011.2000146

[18] Wang, B.; Prester, J. (2025). A labour perspective on videoconferencing fatigue: Critical review and reframing. *The Journal of Strategic Information Systems*, 34, 101903. https://doi.org/10.1016/j.jsis.2025.101903

[19] Ferretti, L.; Magnanini, F.; Andreolini, M.; Colajanni, M. (2021). Survivable zero trust for cloud computing environments. *Computers & Security*, 110, 102419. https://doi.org/10.1016/j.cose.2021.102419

[20] Parast, F.K.; Sindhav, C.; Nikam, S.; et al. (2022). Cloud computing security: A survey of service-based models. *Computers & Security*. https://doi.org/10.1016/j.cose.2021.102580

[21] Ali, S.; Talpur, D.B.; Abro, A.; et al. (2025). Security and privacy in multi-cloud and hybrid cloud environments: Challenges, strategies, and future directions. *Computers & Security*, 157, 104599. https://doi.org/10.1016/j.cose.2025.104599

[22] Akkad, A.; Wills, G.; Rezazadeh, A. (2023). An information security model for an IoT-enabled Smart Grid in the Saudi energy sector. *Computers and Electrical Engineering*, 105, 108491. https://doi.org/10.1016/j.compeleceng.2022.108491

[23] Saeed, S.; Gull, H.; Aldossary, M.M.; et al. (2024). Digital Transformation in Energy Sector: Cybersecurity Challenges and Implications. *Information*, 15, 764. https://doi.org/10.3390/info15120764

[24] Khan, K.A.; Quamar, M.M.; Al-Qahtani, F.H.; et al. (2023). Smart grid infrastructure and renewable energy deployment: A conceptual review of Saudi Arabia. *Energy Strategy Reviews*, 50, 101247. https://doi.org/10.1016/j.esr.2023.101247

[25] Alharbey, R.; Shafiq, A.; Daud, A.; et al. (2024). Digital twin technology for enhanced smart grid performance: integrating sustainability, security, and efficiency. *Frontiers in Energy Research*, 12, 1397748. https://doi.org/10.3389/fenrg.2024.1397748

[26] Khosravi, A.; Sandoval, O.R.; Taslimi, M.S.; et al. (2024). Review of energy efficiency and technological advancements in data center power systems. *Energy and Buildings*, 323, 114834. https://doi.org/10.1016/j.enbuild.2024.114834

UNDER PEER REVIEW IN IJAR

[27] Mytton, D.; Lundén, D.; Malmodin, J. (2024). Network energy use not directly proportional to data volume: The power model approach for more reliable network energy consumption calculations. *Journal of Industrial Ecology*, 28, 966–980. https://doi.org/10.1111/jiec.13512

[28] Zhang, S.; Gao, J.; Qian, H.; Yu, J.; Luo, S.; Guo, Q. (2024). Power system operational reliability assessment based on the data center energy consumption elastic space. *Frontiers in Energy Research*, 12, 1370861. https://doi.org/10.3389/fenrg.2024.1370861

[29] Zygiaris, S.; Maamari, B.E. (2023). The journey from e-government to digital transformation: the case of Saudi Arabia. *Electronic Government, an International Journal*, 19, 95–111. https://doi.org/10.1504/EG.2023.127578

[30] Anh, L.E.T.; Whelan, E.; Umair, A. (2023). 'You're still on mute'. A study of video conferencing fatigue during the COVID-19 pandemic from a technostress perspective. *Behaviour & Information Technology*, 42, 1758–1772. https://doi.org/10.1080/0144929X.2022.2095304

UNDER PEER REVIEW IN IJAR