Session 4 · Computing and Artificial Intelligence for Future Networks

ITU Workshop
Livingstone 2026

Edge Computing Interoperability under African Power Constraints

A Framework for Sovereign Data Residency

Tshiamo Gaborone Khunwane

Founder, Osigak Technologies (Pty) Ltd · EdgeNqoba · Johannesburg, South Africa

Presenting remotely

Presentation Outline

01 **The African Infrastructure Context**
Power constraints, rural connectivity, grid unreliability

02 **Why Edge Computing Is the Strategic Response**
Latency, sovereignty, resilience — the ITU-T Y.3 series rationale

03 **The Interoperability Gap**
Fragmented edge deployments and the absence of African standards

04 **Proposed Framework**
Four-layer architecture for sovereign data residency at the edge

05 **AI-Native Inference Under Constraints**
Power-aware ML at the network edge — design principles

06 **SADC Case Study**
Carrier-grade edge deployment — real implementation lessons

07 **Standards Alignment and Recommendations**
ITU-T Y.3172, Q.3900 series, and the path forward

The African Infrastructure Reality

Power constraints are not a peripheral concern — they define the architecture

600M+
Africans without reliable electricity

32%
Average load-shedding impact on SA operators

$2.8B
Annual African MNO capex on generators

47
SADC licensed MNOs across 16 states

Grid instability forces centralised processing

Edge nodes must operate autonomously during outages. Centralised cloud models fail when the WAN link drops. ITU-T Y.3640 edge computing frameworks assume reliable power — a gap for Africa.

Data sovereignty is physically compromised

When processing occurs off-continent due to power unreliability, subscriber data leaves national jurisdiction. GDPR-equivalent frameworks (Kenya DPA 2019, SA POPIA) require in-country processing.

Carrier-grade SLAs become unachievable

ITU-T G.1010 QoE thresholds for voice and video require sub-50ms local decision latency. Routing to distant cloud infrastructure under congested WAN adds 150–400ms. Edge is not optional — it is required.

Edge Computing as the Strategic Response

ITU-T Y.3 series establishes the theoretical foundation — Africa validates the necessity

ITU-T Framework Alignment	
Y.3172	ML architectural framework in future networks — defines inference at network edge
Y.3173	QoS/QoE assurance for machine learning services in IMT-2020
Y.3640	Edge computing framework and general requirements — reference architecture
Y.3510	Cloud computing requirements and capabilities for network-based data centres
Q.3900	Methods for testing and specification — LI framework for future networks

Edge Value in the African Context

Power autonomy
Edge nodes operate independently during grid outages. Local UPS + solar maintains classification without WAN dependency.

Data residency
Subscriber data processed in-country. Compliant with national data protection legislation. Sovereign by architecture.

Latency guarantee
Sub-1ms local inference vs 150–400ms cloud round trip. ITU-T G.1010 QoE thresholds achievable only at the edge.

Backhaul reduction
Locally-destined traffic steered at the edge. 15–25% reduction in unnecessary WAN transit costs.

Regulatory compliance
Lawful intercept output generated locally. Warrants served without data leaving the national jurisdiction.

The Interoperability Gap

Fragmented edge deployments are creating sovereign data isolation, not integration

Current state: African MNOs deploy edge computing infrastructure from multiple vendors (Huawei, Ericsson, Nokia, open-source) with no common data classification interface, no interoperable LI output format, and no standardised power-aware operational mode. Each deployment is a sovereign island.

No common classification interface

An MNO with Huawei UPF in one corridor and Ericsson UPF in another cannot compare traffic intelligence data. There is no ITU-T standard for encrypted traffic classification output format at the edge.

Impact: Prevents national traffic intelligence aggregation

Power-aware edge operating modes undefined

ITU-T Y.3640 edge computing standards do not define degraded-mode operation for low-power or grid-outage scenarios. African deployments require a 72-hour autonomous operating mode that no current standard addresses.

Impact: Forces vendor-specific implementations

Lawful intercept fragmentation

ETSI TS 102 232 (X3) defines the LI handover interface but not the behavioural enrichment layer for encrypted traffic. Each country implements enrichment differently, creating cross-border coordination problems for SADC regulators.

Impact: Breaks cross-border regulator cooperation

Data residency frameworks absent

No SADC-level framework defines what constitutes sovereign processing at the edge. National data protection laws conflict with federated edge architectures that span multiple jurisdictions.

Impact: Creates compliance uncertainty for operators

Proposed Framework: Four Layers

Sovereign Data Residency at the Mobile Edge — aligned to ITU-T Y.3172 ML architecture

L1

Physical sovereignty layer

Edge node operates within national jurisdiction. UPS + renewable power for 72+ hour autonomous operation. Hardware root-of-trust for data residency guarantee. No data leaves the node without cryptographic authorisation.

ITU-T Y.3640 §6.2 — Edge node physical requirements

L2

Behavioural intelligence layer

AI-native inference operating on behavioural metadata only — not payload. Power-proportional compute: GPU active during peak, ARM-core fallback during load-shedding. Classification output is portable and standard-format.

ITU-T Y.3172 — ML inference at network edge

L3

Compliance and intercept layer

ETSI TS 102 232 X3 output enriched with behavioural context. Warrant-gated LI that never suspends regardless of power state. Cryptographic audit chain for regulatory accountability. Model version tracking for evidence admissibility.

ITU-T Q.3900 series — LI in future networks

L4

Interoperability and corridor layer

Standardised output format consumable by any SADC regulator regardless of underlying vendor. Classification data portable across corridor boundaries. Federated analytics with subscriber-level privacy preservation.

ITU-T Y.2060 · SADC regional cooperation framework

AI-Native Inference Under Power Constraints

Design principles for ML at the African network edge — ITU-T Y.3172 applied

Power-proportional inference architecture — three operating modes

FULL POWER		REDUCED		EMERGENCY	
Hardware:	**GPU + DPU + SmartNIC**	Hardware:	**DPU + SmartNIC (GPU off)**	Hardware:	**SmartNIC only**
Accuracy:	**96%+**	Accuracy:	**88%+**	Accuracy:	**N/A**
Latency:	**<1ms**	Latency:	**<15ms**	Latency:	**Pass-through**
Power draw:	**~400W**	Power draw:	**~120W**	Power draw:	**~40W**
Grid connected. Full XGBoost ensemble on L40S GPU. All features active. Maximum accuracy and throughput.		*UPS power. DPU ARM cores run simplified model. GPU offloaded. Conservative breakout thresholds. LI maintained.*		*Battery / solar minimum. Fail-safe: all traffic forwarded to core. LI mirror rules maintained. No breakout decisions.*	

Core design principle: LI compliance is power-state invariant. Warrant-gated intercept rules are maintained regardless of operating mode. A network node in emergency battery mode must still honour active warrants — this is a legal requirement, not a design choice.

SADC Case Study: Implementation Lessons

Carrier-grade edge intelligence deployment — Botswana corridor, 2026

Context: A national operator with 4.43 million mobile subscribers, 30.1% EBITDA, rural coverage spanning 581,000 km² with variable grid reliability

Lesson 1

GTP-U tunnel layer is the sovereign boundary

Processing at the GTP-U outer header — before decapsulation — captures features unavailable to any post-decapsulation system. This is the only layer where tunnel sequence numbers, timing, and session context are simultaneously accessible. Once decapsulated, this information is permanently lost.

Relevant: ITU-T Y.3172 §5.3 — feature extraction at inference boundary

Lesson 2

Dual-ground-truth for model validation under power constraints

Real-time ground truth from DNS choreography (available in milliseconds) provides a fast drift detection signal independent of the power state. Deep packet inspection ground truth (available in hours) provides confirmed validation. The two-tier approach enables accurate drift detection even during degraded power operation.

Relevant: ITU-T Y.3173 §6.2 — QoS assurance for ML model maintenance

Lesson 3

Regulatory validation must precede commercial deployment

BOCRA LI validation requires 6–9 months. This regulatory timeline is the longest gate in the deployment path — longer than hardware procurement, software development, or commercial negotiation. Operators and regulators must initiate validation simultaneously, not sequentially.

Relevant: ITU-T Q.3900 — LI framework for national regulatory authorities

Lesson 4

Interoperability requires a common output format, not common hardware

SADC corridor interoperability is achievable without replacing existing infrastructure. A standardised JSON classification output format — referencing ETSI TS 102 232 for the LI component — allows any underlying vendor hardware to participate. The interface standard is the enabler, not hardware harmonisation.

Relevant: ITU-T Y.2060 · ETSI TS 102 232 X3 extension fields

Standards Alignment and Recommendations

Where current ITU-T standards apply — and where new work is needed

Existing Standards — Applicable

Y.3172	ML architecture in future networks → Applies to inference engine design
Y.3173	QoS/QoE assurance for ML services → Applies to drift detection framework
Y.3640	Edge computing requirements → Applies to node architecture
Q.3900+	LI in future networks → Applies to intercept output chain
G.1010	End-user multimedia QoS → Applies to QoE classification thresholds

New Work Items Needed

Power-aware edge operating modes
Standard defining 3+ graceful degradation levels for edge AI inference under African grid conditions. Minimum viable LI compliance in each mode.

Encrypted traffic classification format
Common JSON/protobuf schema for behavioural classification output at the edge. Enables vendor-agnostic SADC corridor intelligence federation.

Sovereign data residency attestation
Cryptographic mechanism proving that processing occurred within a specific national jurisdiction. Required for cross-border data protection law compliance.

Post-payload LI enrichment standard
Extension to ETSI TS 102 232 X3 for behavioural context fields: application class, QoE score, model version ID, temporal metadata.

Recommendations to ITU-T and SADC Regulators

Five concrete actions to close the African edge computing interoperability gap

R1	**Initiate new ITU-T work item on power-aware edge AI** SG13 to develop a supplement to Y.3640 covering graceful degradation operating modes for edge computing in power-constrained environments. African and Asian developing nation case studies as primary input.	HIGH
R2	**Standardise encrypted traffic classification output format** SG11/SG13 joint work item: a common format for behavioural traffic classification at the network edge that does not require payload access. Enables SADC corridor intelligence federation without vendor lock-in.	HIGH
R3	**Extend ETSI TS 102 232 X3 for post-payload LI enrichment** ITU-T to engage ETSI LI TC on extension fields for behavioural context in X3 records: application class, model version ID, temporal metadata. Required for evidence admissibility in encrypted traffic cases.	MED
R4	**SADC regional edge interoperability framework** SADC CRASA to develop a regional framework for edge computing interoperability across member state operator networks, with sovereign data residency attestation as a core requirement.	MED
R5	**Establish Africa reference implementation programme** ITU-T AI for Good / Sandbox to support reference deployments of AI-native edge systems in SADC member states, with BOCRA as the first validation authority and the certificate as the regional template.	MED

Key Takeaways

Africa does not need to adapt to global standards.

Africa needs to shape them.

Power constraints define the architecture

Not a limitation to work around — a design input that produces more resilient, sovereign-by-default systems.

The interoperability gap is closeable now

Common output formats, not hardware replacement. This is a standards problem with a standards solution.

Regulatory validation is the long pole

6–9 month LI validation cycles mean operators and regulators must act simultaneously. The clock must start now.

Tshiamo Gaborone Khunwane · tshiamo@afrinnovae.com · osigakgroup.co.za · +27 84 880 8860