Juraj Dobrila University of Pula

Funded by the European Union
NextGenerationEU

Towards an Architecture Theory for Trustworthy Operational Knowledge Construction

Erik Nedeljković, Tihana Galinac Grbac [1]

Juraj Dobrila University of Pula, Zagrebačka 30, HR-52100 Pula, Croatia

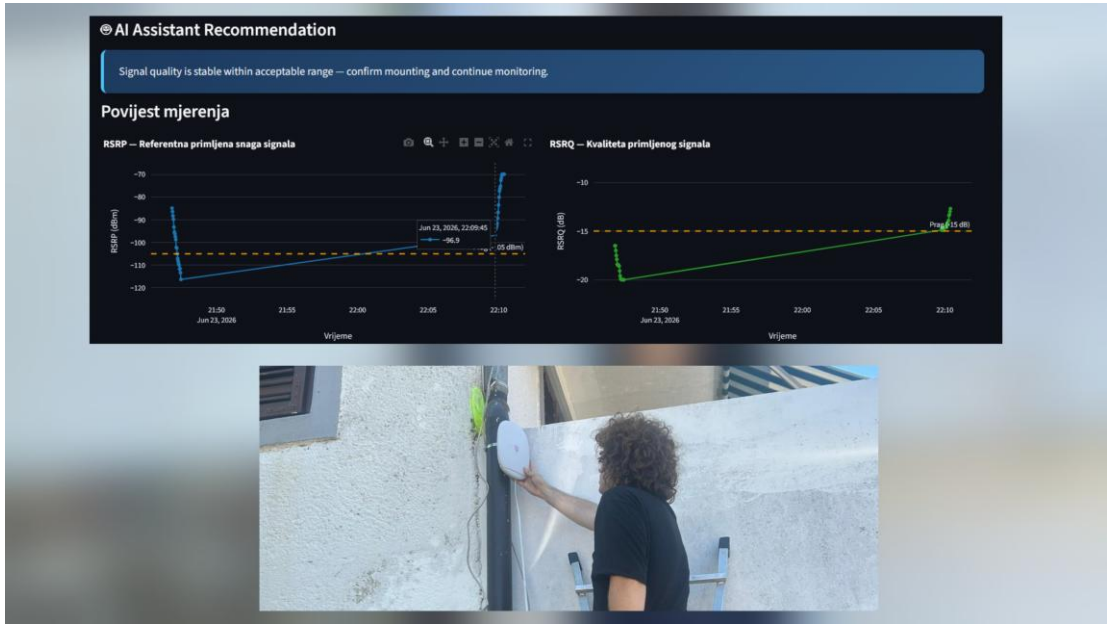
SQAMIA 2026: Workshop on Software Quality Analysis, Monitoring, Improvement, and Applications, September 16–18, 2026, Niš, Serbia

Motivation: Case study from installing 5G antenna

Operational Reality in Cyber-Physical Systems

Digital Representations Decision Making

- Human operators rarely observe physical processes directly.
- Decisions rely on **digital representations** synthesised from heterogeneous sources:
  - Telemetry, sensors, alarm feeds.
  - GIS data, weather conditions, planning models.
  - Historical records & procedural guidelines.
- **Examples**: 5G field service, power grid control, smart water networks, automated manufacturing.



Core Thesis

Software-intensive systems no longer merely process operational data — **they construct the operational situation** upon which human decisions depend.

Problem Statement

Raw observations are incomplete, delayed, or contradictory. Transforming data into trustworthy situational awareness is an **architectural concern**.

The AI Paradox & Architectural Gap

The AI / LLM Opportunity & Risk

- GenAI & LLMs offer powerful semantic reasoning over operational context.
- **Paradox**: AI reasoning quality is strictly bounded by input context quality.
- Naïve AI integration risks hallucinations, unverified advice, and loss of accountability.

Limitations of Existing Frameworks

- **MAPE-K**: Assumes valid runtime knowledge already exists.
- **RAMI 4.0**: Focuses on assets/layers; limited support for human trust/roles.
- **Human-in-the-Loop**: Focuses on UI interaction rather than context construction.

Research Question (RQ)

Which architectural responsibilities are required to construct a trustworthy operational situation for AI-assisted human-in-the-loop decision support?

Paradigm Shift: Situational Awareness as Emergent Quality

Endsley's Cognitive SA Model

1. **Level 1: Perception** of relevant environmental elements.
2. **Level 2: Comprehension** of their operational meaning.
3. **Level 3: Projection** of future system state.

SA is traditionally viewed as a human cognitive trait, not a software specification.

Proposition 1

Operational Situational Awareness is an **emergent architectural quality** arising from the coordinated execution of architecturally significant responsibilities that construct trustworthy operational context.

Architectural Implication

SA is not a single button or AI module; it emerges from system-wide architectural capabilities.

Deductive Architectural Derivation Method

Failure-Oriented Architectural Reasoning Chain:

Operational Objective → Architectural Concern → Failure Mode → Capability → Responsibility

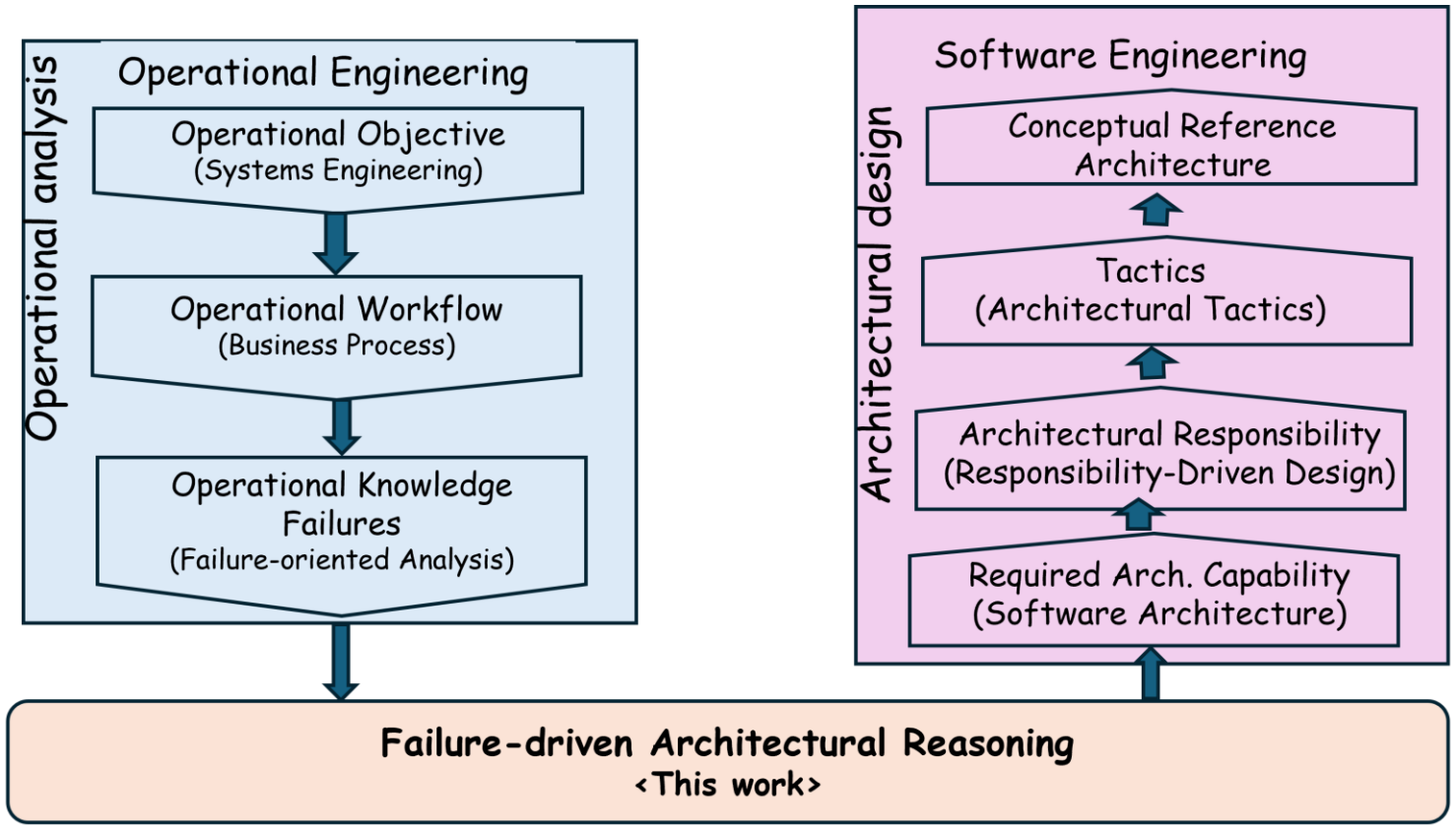
Methodological Rationale

- Instead of intuiting software components, we ask: *"What operational failure modes prevent trustworthy decisions?"*
- Each failure mode exposes a required persistent capability.
- Capabilities are formalised into stable, technology-independent responsibilities.

Derivation Traceability

- Ensures 100% traceability from high-level operational objectives to architectural design decisions.
- Technology-independent: LLMs, Rule Engines, or Knowledge Graphs can realise individual responsibilities.

Failure-driven reasoning process (FDRP)



Transforms Operational Knowledge Failures into Architectural Design Decisions

Case Study: 5G Coverage Verification & Commissioning

Operational Scenario

- Field engineer verifies 5G outdoor antenna coverage post-installation.
- Heterogeneous Inputs: RSRP, RSRQ, SINR telemetry, Cell ID, GIS topography, weather, operator thresholds.
- Objective: Determine optimal antenna tilt/azimuth or accept installation.

Field Realities

Unstable remote network connectivity, high telemetry volume, manual measurement errors.

LLM-Augmented MAPE-K Loop

- **Monitor**: Telemetry acquisition & local filtering.
- **Analyze/Plan**: LLM converts telemetry → natural language intent recommendations.
- **Offline-First**: Local buffer preserves context during connection dropouts; syncs asynchronously.
- **Human-in-the-Loop**: Technician reviews, deliberates, and executes final physical adjustment.

M. Ghassemian, P. Muschamp and D. Warren, "Experience Building a 5G Testbed Platform," 2020 IEEE 3rd 5G World Forum (5GWF), Bangalore, India, 2020, pp. 473-478.

Workflow Activity	Required Operational Knowledge	Operational Knowledge Failure	Possible Cause	Operational Consequence
Site survey and planning	Deployment constraints, environmental context, expected coverage	Incomplete operational context	Missing environmental information, outdated planning assumptions	Incorrect deployment assumptions
Installation and configuration	Current deployment state and configuration	Configuration mismatch	Provisioning errors, incomplete topology discovery	Incorrect diagnosis of deployment problems
Coverage verification	Correct interpretation of field measurements	Incorrect interpretation of observations	Reflection, shadowing, incomplete context	Wrong corrective action
Operational interpretation	Integrated operational understanding	Unsupported operational explanation	Single hypothesis, insufficient evidence	Incorrect operational recommendation
Decision making	Justified operational recommendation	Recommendation not sufficiently justified	Missing evidence, low confidence, conflicting observations	Incorrect field intervention
Operational adaptation	Updated operational knowledge	Operational learning not preserved	Missing feedback integration	Repeated operational errors

Operational Knowledge Failure	Required Architectural Capability	Derived Architectural Responsibility
Incomplete operational context	Acquire and synchronise relevant operational evidence; assess its provenance, freshness, and reliability	Context Acquisition; Trust Assessment
Configuration mismatch	Maintain an explicit and current representation of the actual runtime configuration and operational state	Runtime Operational Knowledge Management
Incorrect interpretation of observations	Detect inconsistencies among heterogeneous observations and integrate available evidence into a coherent operational representation	Context Validation; Context Integration
Unsupported operational explanation	Generate and evaluate alternative explanations using available operational evidence	Operational Reasoning
Recommendation not sufficiently justified	Assess evidence sufficiency, uncertainty, constraints, and expected consequences; expose the recommendation rationale and support human assessment	Decision Assurance; Intent and Explanation Generation; Human Deliberation Support
Operational learning not preserved	Capture outcomes of operational actions and incorporate them into evolving operational knowledge	Knowledge Evolution

Layered Responsibility Decomposition

Layered Responsibility Decomposition

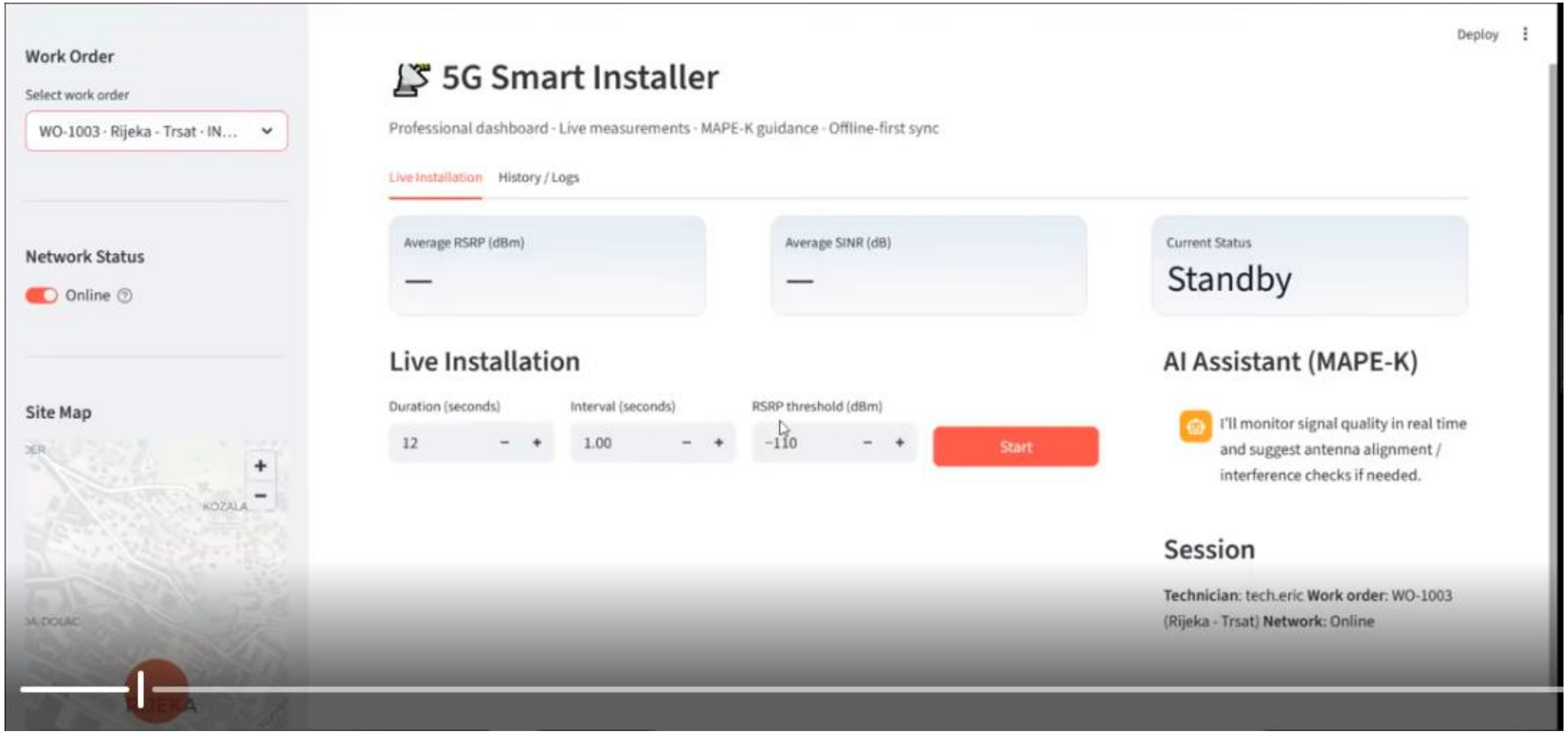
1. **Layer 5: Intent & Human Interaction**: Intent Generation, Interactive Deliberation, Human Decision.
2. **Layer 4: Operational Reasoning & Assurance**: Adaptive Reasoning (LLM), Decision Assurance.
3. **Layer 3: Runtime Knowledge Management**: Runtime Operational Model (Models@Runtime / Digital Twin).
4. **Layer 2: Operational Context Management**: Acquisition, Trust Assessment, Validation, Integration.
5. **Layer 1: Execution & Control**: Execution Workflow, Feedback Loop.

Key Invariant

Separation of Concerns: Context construction is strictly separated from LLM reasoning and human oversight.

Architectural Decisions and Tradeoffs

Architectural Decision	Motivation & Quality Attribute	Architectural Rationale
Human-on-the-loop Authority	Safety, Accountability, Compliance (EU AI Act)	AI recommends; human holds final decision authority.
Technology Independence	Modularity, Maintainability	LLM is pluggable; replaceable by Rule Engine or KG.
Offline-First Persistence stalling in remote field locations.	Availability, Resilience	Prevents data loss
LLM in Analyze/Plan Stages	Separation of Concerns	LLM performs semantic translation, not raw data ingestion.


Deploy
5G Smart Installer
Professional dashboard - Live measurements · MAPE-K guidance · Offline-first sync
Live Installation
History / Logs
Work Order
Select work order
WO-1003 · Rijeka - Trsat · IN...
Network Status
Online
Site Map
Average RSRP (dBm)
—
Average SINR (dB)
—
Current Status
Standby
Live Installation
Duration (seconds)
12
Interval (seconds)
1.00
RSRP threshold (dBm)
-110
Start
AI Assistant (MAPE-K)
I'll monitor signal quality in real time and suggest antenna alignment / interference checks if needed.
Session
Technician: tech.eric Work order: WO-1003 (Rijeka - Trsat) Network: Online
KOZALA

Deploy

Work Order

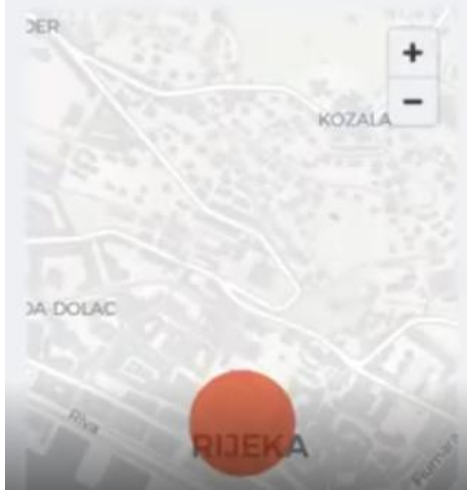
Select work order

WO-1003 · Rijeka - Trsat · IN…

Network Status

Online

Site Map



—

—

Standby

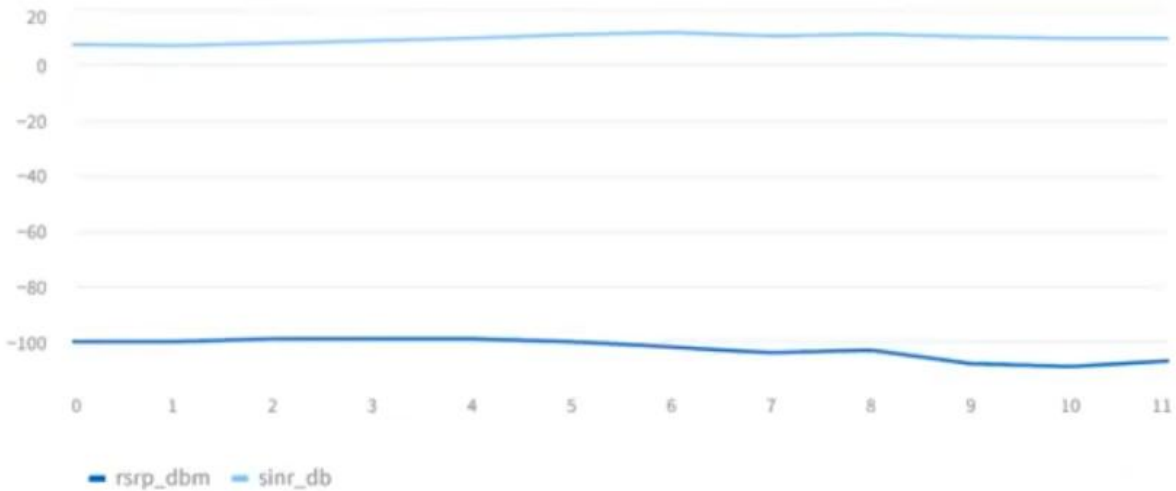
Live Installation

Duration (seconds) 12 − +

Interval (seconds) 1.00 − +

RSRP threshold (dBm) −110 − +

Start



MAPE-K: OK · avg RSRP -106.2 dBm · avg SINR 10.2 dB

Sample 12/12 · RSRP -107 dBm · SINR 9.6 dB · 11:59:39

AI Assistant (MAPE-K)

I'll monitor signal quality in real time and suggest antenna alignment / interference checks if needed.

Signal looks stable. Continuing monitoring…

Recommendations

- (none yet)

Session

Technician: tech.eric **Work order**: WO-1003 (Rijeka - Trsat) **Network**: Online

Report Summary

Deploy

5G Smart Installer

Professional dashboard · Live measurements · MAPE-K guidance · Offline-first sync

Live Installation | History / Logs

Work Order

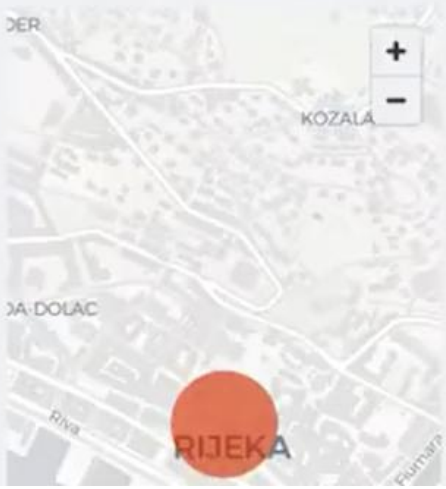
Select work order

WO-1003 · Rijeka - Trsat · IN…

Network Status

Online

Site Map



History / Logs

Local offline-first storage (from the same `local_db.json` used by `LocalDatabase`).

Reports in history	Pending sync queue
2	0

report_id	work_order_id	location	technician	started_ts	finished_ts	sync	recommendations
RPT-1777291179-750	WO-1003	Rijeka - Trsat	tech.eric	2026-04-27T11:59:21.958913+00:00	2026-04-27T11:59:39.225015+00:00	☑	0
RPT-1777287117-201	WO-1001	Zagreb - Maksimir	tech.eric	2026-04-27T10:51:42.482931+00:00	2026-04-27T10:51:57.389989+00:00	☑	0

Scenario-Based Evaluation & Insights

Evaluated Scenarios

- **Scenario A**: Stable connectivity, nominal telemetry.
- **Scenario B**: Temporary network blackout (Offline buffer test).
- **Scenario C**: Degraded / weak signal measurements.
- **Scenario D**: Contradictory neighbour cell observations.

Key Evaluation Findings

- **Resilience**: Offline-first pattern maintained operational continuity without data loss.
- **Trust Calibration**: Intent layer significantly reduced cognitive load vs. raw RSRP analysis.
- **Safety**: Decision Assurance prevented hallucinated or policy-defying tilt actions.

Summary & Key Takeaways

1. Context First

Operational situation construction **must precede** AI reasoning. AI cannot fix corrupted context.

2. Emergent SA

Situational awareness is an **emergent architectural quality**, not a single component.

3. Human Authority

Explicit responsibilities preserve **human oversight, safety, and accountability**.

Thank You!

Questions & Discussion

Paper: Architectural Responsibilities for AI-Assisted Operational Situation Construction: A 5G Field Installation Case Study
Conference: SQAMIA 2026

This work is supported by the EU NextGeneration under the Juraj Dobrila University of Pula institutional research project EQUYSIS – Human-Centered System Design for Equitable and Sustainable Digital Societies, project number IIP_UNIPU_010162.

We invite you to submit a paper to

SSE - Software and Systems Engineering

Important dates:

Abstract submission deadline: Monday, October 19, 2026
Full paper submission deadline: Monday, November 30, 2026
Final paper review deadline: Monday, February 01, 2027