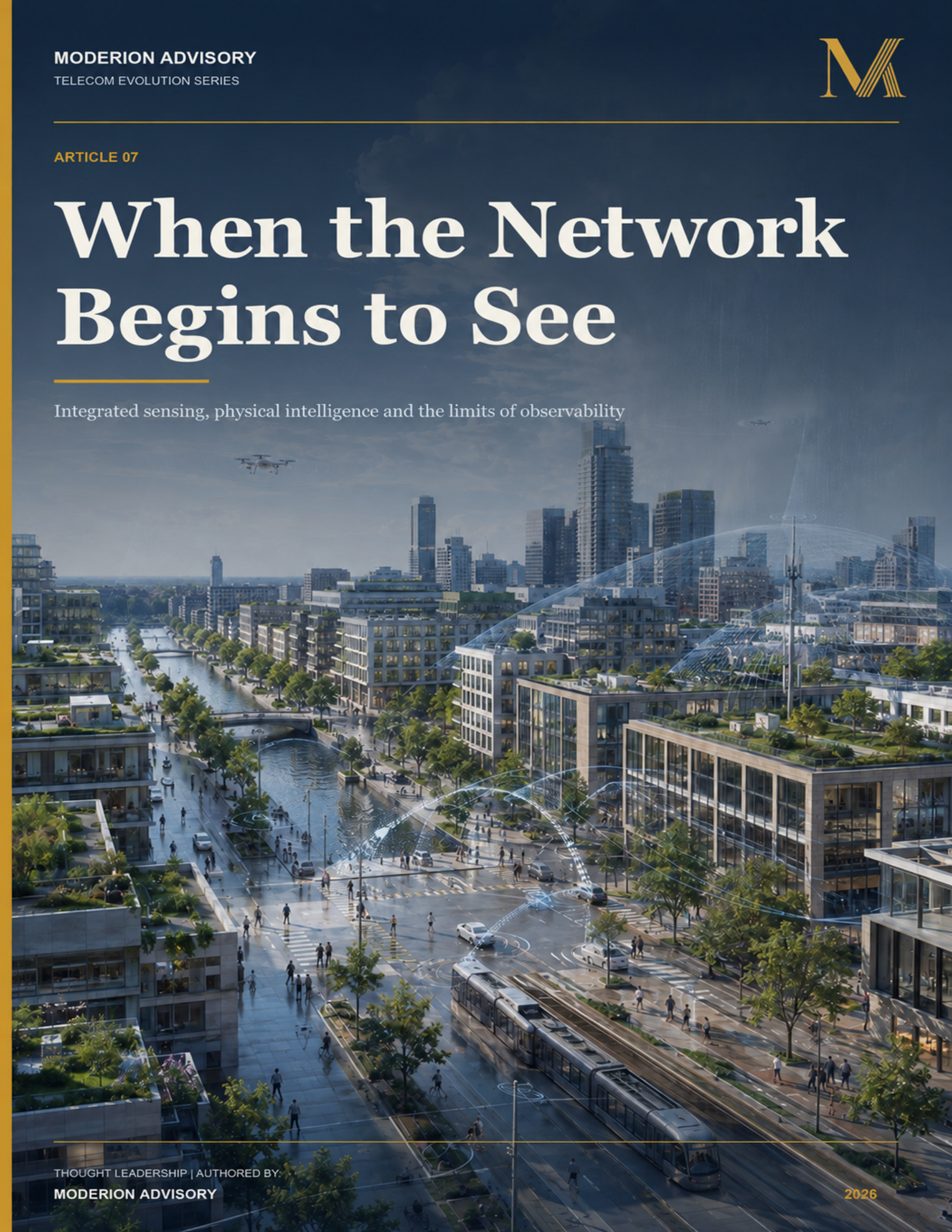


ARTICLE 07

When the Network Begins to See

Integrated sensing, physical intelligence and the limits of observability



When the Network Begins to See

Integrated sensing, physical intelligence and the limits of observability

AUTHOR Moderion Advisory

SERIES The Total Connectivity Economy

EVIDENCE CURRENT TO 6 September 2026

EXECUTIVE PROPOSITION

Integrated sensing and communication can turn network infrastructure into a distributed physical-intelligence layer. Its legitimacy and economics will depend on accuracy, consent, purpose limitation, liability and a clear buyer - not on sensing capability alone.

Executive summary

Integrated sensing and communication can turn network infrastructure into a distributed physical-intelligence layer. Its legitimacy and economics will depend on accuracy, consent, purpose limitation, liability and a clear buyer - not on sensing capability alone.

This evidence-led thought article develops an executive point of view using standards, official data, company disclosures and Moderion Advisory analysis. It separates established facts from emerging direction and reported implementation.

EXECUTIVE QUESTION

What changes when radio infrastructure becomes a sensing system for unconnected objects and physical environments?

Key insights at a glance

- ITU-R M.2160 identifies integrated sensing and communication as an IMT-2030 usage scenario, including object detection, localization, imaging, mapping, activity recognition and environmental monitoring.
- ISAC can reuse spectrum, sites, waveforms and signal processing, but communications coverage does not automatically equal validated sensing coverage or accuracy.
- Commercial value depends on a complete sensing product: measured object, accuracy, refresh rate, confidence, geographic boundary, permitted purpose and accountable response.
- The strongest near-term cases are likely to be bounded environments with a responsible operator and observable ground truth: industrial sites, transport corridors, ports, campuses and critical infrastructure.
- Sensing unconnected people or objects creates a different legitimacy burden from carrying user-requested communications. Notice, consent or lawful basis, retention, access, bias, redress and misuse controls must be designed before scale.
- Liability is central. A probabilistic inference should not silently become a safety-critical instruction; decision rights must reflect confidence and consequence.
- ISAC is a resource-allocation problem as well as a waveform opportunity. Sensing accuracy, communications throughput, coverage, energy, compute and privacy objectives must be optimized together.

- ITU's emerging framework introduces authentication of sensing requests, capability discovery, sensing-node selection, multi-site processing and controlled exposure of sensing results.
- Commercial readiness depends on a bounded accuracy envelope and a named liability owner; object detection or tracking claims without probability of detection, false-alarm rate, resolution and environmental conditions are not bankable products.
- This article contributes to the Total Connectivity Economy by testing its enabling mechanism against universal reach, open interoperability, governed intelligence, trusted participation and sustainable economics.
- A 2025 IEEE Communications Surveys & Tutorials review documents architectures, prototypes and testbeds while retaining major open issues; it supports ISAC's technical seriousness but not ubiquitous production readiness.
- ITU-T's November 2025 technical report treats authentication, request lifecycle, node selection, measurement processing and controlled result exposure as core framework requirements, reinforcing the article's governance-first position.

Exhibit 1 | ISAC value-and-risk chain

Stage	Output	Control question
Sense	Radio observations	Was collection authorized and bounded?
Infer	Object / event estimate	What is the calibrated uncertainty?
Fuse	Contextual picture	What sources and biases shaped it?
Decide	Recommended action	Who owns the consequence?
Act	Physical / operational response	Can the action be stopped or challenged?

Note: Moderion Advisory assurance chain.

Exhibit 3 | ISAC product assurance envelope

Dimension	Measure	Why it matters	Commercial control
Detection	Probability of detection / false alarm	Reliability of event	Minimum threshold and test set
Resolution	Range, velocity and angle error	Usable decision precision	Published operating envelope
Communications	Throughput, latency and energy impact	Shared-resource cost	Capacity reservation and priority
Environment	Weather, clutter, geometry and load	Generalizability	Scenario qualification
Governance	Purpose, retention and access	Privacy and accountability	Auditable request and result

Note: A sensing SLA is multidimensional; headline accuracy without operating conditions is not sufficient evidence.

Core analysis

A change in the network's purpose

Mobile systems have traditionally carried information and estimated device position. IMT-2030 frameworks add integrated sensing and communication as a new usage scenario. Radio signals may be used to detect, range, track or characterize objects and environments through their propagation and reflections. Infrastructure built for communication could therefore contribute to mobility management, weather observation, industrial safety, infrastructure monitoring and digital twins.

This is a major expansion of institutional power. A network that can observe physical activity is not merely a better pipe. It becomes part of the sensing environment. The technical design must therefore be developed together with legal authority, social legitimacy and service accountability.

Capability and maturity

Research demonstrates promising techniques across radar-like sensing, localization and joint waveform design, but performance varies with frequency, geometry, density, obstruction and environmental conditions. Laboratory accuracy cannot be generalized to every public environment. Communication and sensing objectives may also compete for spectrum, energy and network resources.

The relevant maturity ladder runs from simulated feasibility to controlled testbed, field trial, specified capability, lawful service and scaled commercial operation. Claims should state where they sit on that ladder. The industry should resist presenting pre-standard research as a finished 6G product.

The governance architecture

Purpose limitation is foundational. A system approved for traffic optimization should not silently become a general surveillance platform. Data minimization, aggregation, retention limits and access controls must be defined by use case. Where individuals or private premises may be observed, consent, legal basis and redress become central. Model outputs need confidence estimates and audit trails because sensing errors can create physical or legal consequences.

Liability must also be allocated. If a sensing service fails to detect a hazard, misclassifies an object or feeds an unsafe automated decision, responsibility may span operator, vendor, application provider and customer. Service definitions must distinguish raw measurement, inferred event and guaranteed outcome.

Where a market may emerge

The most credible early markets are environments with a defined asset owner, bounded geography and measurable outcome: ports, factories, campuses, transport corridors, utilities and critical infrastructure. Public-space applications may offer broad social value but face more demanding legitimacy and procurement tests. In every case the buyer must value the network's coverage, synchronization or integration advantage relative to cameras, radar, lidar and dedicated sensors.

A sustainable product will combine sensing with communications, edge compute, analytics and operational workflow. Selling raw observations is less defensible than improving a specific safety, maintenance or logistics outcome under clear governance.

Moderion Advisory perspective

From radio reflection to accountable information

The technical pipeline includes waveform and resource allocation, propagation, reflected-signal capture, feature extraction, inference, fusion and application action. Error can enter at every stage. Weather, movement, occlusion, material, geometry and interference may alter the signal. A commercial service therefore needs calibrated uncertainty, not only a point estimate.

Performance should be reported against use-case ground truth using detection probability, false alarm rate, localization error, refresh interval, coverage and stability across operating conditions. Demonstrations without these measures establish possibility, not operational fitness.

A legitimacy architecture

The sensing service should be purpose-bound. The entity authorizing the use, operating the network, building the model, receiving the data and acting on it may be different. Contracts and technical controls must assign each responsibility and prevent secondary use that exceeds the approved purpose.

High-consequence use should retain human or certified-system review, preserve evidence and offer a path to challenge. Privacy protection should include minimization at source, restricted resolution where possible, short retention, role-based access and audit. These are product requirements, not post-launch compliance tasks.

How a communication waveform becomes a sensing instrument

OFDM signals provide structured time-frequency resources that can support estimation of delay, Doppler and angle when transmitted and reflected paths are observed. Range relates to propagation delay, radial velocity to Doppler shift, and direction to phase differences across antenna elements. Performance depends on bandwidth, carrier frequency, aperture, signal-to-noise ratio, waveform occupancy, synchronization, geometry and the surrounding multipath environment.

The operator cannot assume sensing is free. Reserving symbols, pilots, bandwidth, antennas or compute may affect communications capacity or energy. Conversely, communications traffic and infrastructure can improve sensing coverage and economics. The design target is a Pareto frontier: the set of configurations where one objective cannot improve without reducing another. Product promises should be selected from measured points on that frontier.

Three commercial blueprints

For an urban-air-mobility corridor, network sensing can complement cooperative transponders by detecting and tracking objects within a defined volume; the authority still needs identification, fusion and air-traffic rules. In a smart port, sensing can support berth occupancy, vehicle movement and restricted-zone monitoring when fused with cameras, radar and logistics systems. For critical-perimeter monitoring, the service can provide presence or trajectory alerts, but must expose confidence and environmental limitations.

Each product needs a requester, sensing-area authorization, node-selection policy, accuracy envelope, retention rule, fusion architecture, incident workflow and commercial remedy. The service should sell an assured decision input, not claim that radio reflections replace certified safety systems.

Privacy, safety and evidential governance

Passive sensing can reveal movement or behavior even when the observed person carries no connected device. Governance must therefore begin with identifiability and purpose, not with whether a subscriber record exists. Controls include geographic and temporal minimization, resolution limits, role-based access, aggregation, retention limits, model and sensor provenance, and independent audit for sensitive deployments.

A sensing request should be authenticated and authorized; the selected nodes and processing purpose should be logged; raw measurements should be separated from derived events; and uncertainty should travel with the result. Where outputs influence safety, security or enforcement, a human-review and contestability route is required unless law and validated engineering support a different control model.

Sensing expands participation and responsibility

Integrated sensing can make connectivity context-aware, but it also observes people and environments that may never have consented as subscribers. Its contribution to the North Star therefore depends on bounded purpose, declared accuracy, proportionality, retention control, contestability and clear liability. Communications infrastructure may augment dedicated sensors; it does not automatically replace safety-certified systems.

The boundary between sensing capability and sensing service

The literature now provides credible technical architectures and increasingly sophisticated testbeds. Commercial evidence remains sparse because accuracy, false alarms, environmental robustness, privacy, liability and a responsible operational response must be proven together.

The article therefore avoids the claim that communications infrastructure will replace dedicated safety-critical sensing. ISAC is best treated as an additional, potentially powerful sensing modality whose fitness must be validated against the decision and consequence at hand.

Exhibit 2 | Evidence required by use-case consequence

Consequence	Example	Minimum evidence
Low	Anonymous occupancy trend	Aggregate accuracy and privacy control
Material	Traffic or logistics optimization	Condition-specific validation and monitoring
High	Safety, defense or enforcement action	Certified performance, chain of custody and accountable review

Note: Requirements must be adapted to applicable law and sector regulation.

Executive action agenda

- Classify sensing claims by maturity and publish the conditions under which accuracy was achieved.
- Define purpose, lawful basis, retention, access, confidence and redress before field deployment.
- Separate measurement, inference and guaranteed outcome in technical and commercial contracts.
- Prioritize bounded enterprise environments with accountable buyers and measurable benefits.
- Create joint technical, legal, safety and ethics governance for every sensing product.

Conclusion

A network that begins to see can create genuine public and enterprise value, but observability is not automatically legitimacy. The industry's responsibility is to make sensing bounded, auditable and useful. The commercial opportunity will follow only where that responsibility is designed into the service from the beginning. In the wider series, this capability is treated as an enabler of the Total Connectivity Economy rather than as an end state in itself.

Selected evidence and references

- T001 | ITU-R. Framework and overall objectives of the future development of IMT for 2030 and beyond. 2023. ITU Recommendation M.2160-0. <https://www.itu.int/rec/R-REC-M.2160-0-202311-I>
- T029 | Liu et al.. Integrated Sensing and Communications: Toward Dual-Functional Wireless Networks for 6G and Beyond. 2022. IEEE Journal on Selected Areas in Communications. <https://ieeexplore.ieee.org/document/9737357/>
- T030 | Multiple authors. Advanced Learning Algorithms for ISAC Systems in 6G and Beyond: A Comprehensive Survey. 2025. IEEE Communications Surveys & Tutorials. <https://ieeexplore.ieee.org/document/11062661>
- T031 | Multiple authors. A Survey on Integrated Sensing and Communication With Intelligent Metasurfaces. 2025. IEEE Open Journal of the Communications Society. <https://ieeexplore.ieee.org/document/11111722/>
- T032 | Multiple authors. Ten challenges in semantic communications. 2025. China Communications. <https://ieeexplore.ieee.org/document/11045871/>
- T037 | Bronwyn Howell. Beyond infrastructure: Internet ecosystem resilience and the public good. 2025. Telecommunications Policy. <https://www.sciencedirect.com/science/article/pii/S0308596125000953>
- P031 | 3GPP. 5G-Advanced Maturity. 2025. 3GPP Highlights Issue 11. https://www.3gpp.org/images/newsletters/3GPP_Highlights_Issue_11_FLIPBOOK.pdf
- P032 | 3GPP. 3GPP Workshop on 6G — Contribution Index. 2025. 6G Workshop 2025. https://www.3gpp.org/FTP/Meetings_3GPP_SYNC/Workshop/Docs
- ITU-R. Recommendation M.2160-0, integrated sensing and communication. https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2160-0-202311-I!!PDF-E.pdf
- ITU-T. Work programme: requirements and framework for ISAC. https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=13&wp=1
- IEEE Communications Surveys & Tutorials. Integrated sensing and communications research corpus (refer to the paper bibliography for selected peer-reviewed surveys).
- ITU-T. YSTR.ISAC-fra: Considerations on integrated sensing and communication in IMT-2020 networks and beyond (2025). <https://www.itu.int/publications/publication/itu-t-ystr-isac-fra-2025-11-considerations-on-integrated-sensing-and-communication-in-imt-2020-networks-and-beyond>

ITU-T Study Group 17. Security guidelines for ISAC work programme. https://www.itu.int/itu-t/workprog/wp_search.aspx?sg=17&wp=2

PR022 | ISAC - A Survey on Its Layered Architecture, Technologies, Standardizations, Prototypes, and Testbeds. IEEE Communications Surveys & Tutorials 28, 485-526 (2025). <https://doi.org/10.1109/COMST.2025.3565534>

PR023 | Advanced Learning Algorithms for Integrated Sensing and Communication Systems in 6G and Beyond. IEEE Communications Surveys & Tutorials 28, 2572-2611 (2025). <https://doi.org/10.1109/COMST.2025.3584333>

PR024 | ITU-T. YSTR.ISAC-fra: Considerations on integrated sensing and communication in IMT-2020 networks and beyond (2025). <https://www.itu.int/pub/T-TUT-IMT-2025-1>