5G-Advanced Core

Test and assurance strategies for unlocking monetization

eBook

KEYSIGHT

Introduction

The first wave of 5G deployments laid the foundation for modern mobile connectivity.

Built on 3GPP Releases 15–17, software-driven, cloud-native, and flexible networks defined a new era of telecom service delivery. However, monetization of associated speed and capacity gains has proven elusive, with commercial service innovation occurring at a slower than expected pace.

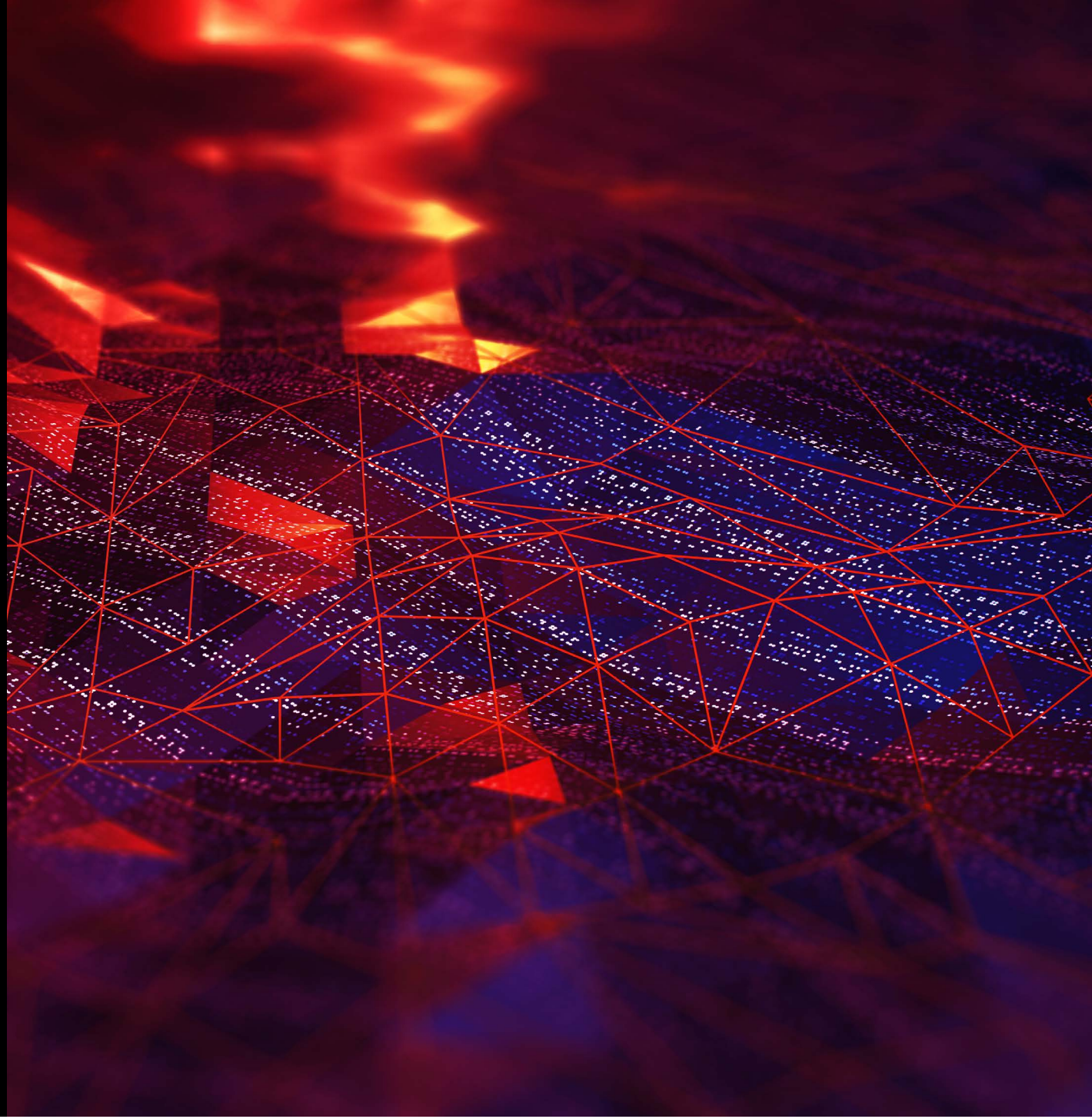
Now, 5G-Advanced (5G-A) promises to transform 5G networks into smarter, revenue-generating platforms readily able to serve the requirements of a broader, more demanding customer base. It also integrates artificial intelligence (AI) and machine learning (ML) directly into network architecture — laying the essential groundwork for truly autonomous networks. This advancement will simultaneously raise the stakes for consistent, measurable performance and governance, making test and assurance central to delivering on 5G-A's full promise.

Contents

5G

CHAPTER 1

What is 5G-Advanced?



CHAPTER 1

What is 5G-Advanced?

Defined by 3GPP Releases 18–20, 5G-A marks a shift to advanced, high-value services delivery at scale by extending current 5G architectures with features that unlock ultra-reliable low-latency communication (URLLC), add intelligence, adaptability, and commercial viability in every network layer, from the air interface to the core.

The result is meaningful improvements to capabilities like network slicing, tighter integration of AI/ML in the radio access network (RAN) and core, and more efficient Internet of Things (IoT) and industrial use case support. Connectivity options also get a boost via satellite and non-terrestrial networks (NTN).

As noted in Keysight's 2025 5G Report, planned advancements align with monetizable use cases across a diverse set of verticals, including manufacturing, transportation, logistics, energy, public safety, and more. In short, they position 5G as a high-performance and differentiated platform, built on 5G standalone (SA) architecture with a cloud-native core that enables intelligent service delivery, edge offload, and deeper automation.

3GPP timeline: understanding the release roadmap

Each remaining 3GPP release planned for 5G will build toward a more intelligent, versatile, and commercially viable 5G system:

Release 18 is frozen, marking the start of practical deployment planning for many of the enhancements noted above, including expanded vertical support and greater core and RAN flexibility.

Release 19 is in development and expected to extend this momentum with deeper support for AI-driven operations, IoT, and use cases at the edge.

Release 20 will further expand capabilities while beginning to bridge toward 6G.

This release cadence is both a technical roadmap and a planning tool, with anticipated feature availability ultimately shaping decisions around how and when to design test coverage, validate service behaviors, and operationalize assurance strategies. This exercise is critical for ultimately translating advanced network features into revenue-generating services.

	R18	*R19*
	Low-power high-accuracy positioning for industrial IoT eRedCap devices for further complexity reduction Slice enhancements, including temporary and area of service	Edge computing for industrial scenarios (security, digital twins) Ambient IoT (study item)
	NTN transparent mode enhancements, including L/S band	NTN regenerative mode, enhanced DL/UL and RedCap support
	NR sidelink evolution (CA, unlicensed spectrum, relay)	NR sidelink multi-hop relay
	Interconnection and migration aspects for Future Railway Mobile Communication System (FRMCS)	FRMCS phase 5, smart stations (study item)
	XR+media enhancements for traffic awareness & QoS	XR+M enhancements for Metaverse
	NR support for UAVs	Architecture enhancements for UAVs (security)
AI	AI/ML for NG-RAN incl. data collection and signaling support	AI/ML for NG-RAN enhancements (beam mgt, positioning) AI/ML for NR air interface, mobility, and slicing (study items)

The strategic opportunity for operators

Operators view 5G-A as an opportunity to reframe the value of next-generation networks, anchored in performance and enterprise-grade feature advancements. Whereas 5G delivered general connectivity improvements, 5G-A specifically targets tightly defined services that require position, control, and guaranteed outcomes.

For enterprise customers in a range of verticals, 5G-A can transform private network deployments, industrial IoT capabilities, and time-sensitive communications. Services like more granular network slicing, edge integration, mission-critical communications, and improved device energy efficiency, are set to power use cases like smart factories, logistics hubs, or automated transport systems.

For consumers, 5G-A promises to provide more immersive experiences as XR-ready network functions, satellite integration for remote coverage, and dynamic QoS management enable premium service differentiation and expansion of service into underserved areas.

> 5G-Advanced turns the 5G core into a revenue engine — enabling programmable control, real-time analytics, and premium services for enterprises and consumers alike.

Monetization opportunities are buoyed by new levers like expanded exposure functions, real-time analytics, and more programmable control with the 5G core becoming a revenue engine in its own right. This positions developers, enterprises, and partners alike to build value on top of the network, supporting a robust ecosystem driven by a common growth engine.

Test and assurance in the 5G-A era

It is important to note that as operators deploy new features, they are also promising new business outcomes.

5G-A introduces new services, behaviors, and expectations that demand consistent testing, validation, and assurance capabilities that must be met in the lab and live, dynamic environments. Traditional test methods fall short on this front as assurance can no longer be a one-time checkpoint but rather a continuous, closed-loop discipline spanning development, deployment, and operations.

Whether validating slicing logic or edge offload performance to ensure buffer behavior during satellite handovers, test assurance strategies must evolve in lockstep with 5G-A capabilities. This eBook explores supporting methodologies, outlining how operators can apply emulation, CI/CD pipelines, and active testing to de-risk deployments, guarantee service quality, and support trusted, revenue-ready offerings.

CHAPTER 2

Operator Value in Release 18

CHAPTER 2

Operator Value in Release 18

5G-Advanced Release 18 takes the first step toward making 5G networks more programmable, responsive, and aligned to real-world service demands.

This release delivers practical features that can support new revenue models, more tailored enterprise offerings, and richer consumer experiences. It also builds on earlier releases with targeted updates for extended reality (XR), positioning, and energy efficiency, expanding the foundation for vertical and industrial use cases with:

Enhanced support for industrial services such as automotive V2X, uncrewed aerial vehicles (UAVs), railways, private 5G networks, edge computing, and ultra-reliable low latency communications

Efficiency improvements for IoT, including enhancements to eRedCap and machine-type communication (MTC), and extended coverage via satellite integration

Broader coverage and richer consumer experiences via improved non-terrestrial networks integration

New monetization opportunities powered by dynamic network slicing, QoS-based service tiers, and advanced data exposure frameworks

Higher network efficiency and performance across RAN and core layers

Expanded support for sidelink, proximity services, location awareness, and high-accuracy positioning

Multicast and broadcast services (MBS) for scalable content distribution and group communication use cases

In addition to expanded service coverage and new monetization opportunities, Release 18 introduces foundational enablers to improve how these services are delivered and optimized. This includes AI/ML playing a more direct role in the RAN and core via smarter resource allocation and more adaptive performance management.

Immersive communications like XR, augmented reality (AR), and virtual reality (VR) can also improve network responsiveness and application-aware quality of service. Enhancements to edge computing move compute closer to the user for low-latency processing across industrial control, XR rendering, and real-time analytics.

Operational efficiency gains are a result of these advancements, as automation, advanced analytics, and energy-saving capabilities are integrated throughout the system. In short, Release 18 gives operators more tools to manage complexity, reduce OpEx, and support sustainable growth.

Release 18 also extends new value across enterprise, industrial, and consumer markets by helping operators turn advanced network features into differentiated offerings and new sources of revenue.

Expansion across enterprise and vertical markets

Release 18 streamlines private 5G non-public networks (NPN) deployments including partial-slice coverage, non-3GPP access, and increased security integration. This enhances the operator's ability to offer fully managed private networks to factories, campuses, mines, and more, unlocking new B2B service revenue. Edge computing integration offers enhanced local breakout and traffic steering allowing operators more control in placing compute resources near enterprises for real-time analytics, augmented reality / virtual reality, or near-zero latency control loops. Operators can package these edge capabilities as premium services for industrial or enterprise customers.

Deeper support for IoT and industrial automation

Release 18 introduces enhanced reduced capability (eRedCap) supporting lighter, cheaper modules that enable more IoT deployments (sensors, cameras, wearables), with connection plans sold by operators. Time-sensitive networking (TSN) and ultra-low latency enhancements allow operators to interwork with factory or utility local area networks (LANs), fine tune uplink and downlink latency, and provide tight cross-layer coordination to offer slice-level guaranteed performance. Enhanced uncrewed aerial vehicle (UAV) support allows operators to serve new business lines for aerial services, from agriculture to security.

Advanced consumer services

Release 18 supports satellite and NTN coverage expansion allowing operators to serve messaging, voice, and broadband connectivity in remote areas, maritime shipping routes, or emergency scenarios, significantly broadening coverage footprints. XR (AR/VR) is enhanced through upgrades across the 5G core and RAN, enabling low-latency, high-throughput experiences and allowing operators to partner with content providers to offer premium consumer packages.

Enhanced slicing and QoS

Release 18 provides operators enhanced slice coverage and control, including partial slice geographical coverage (key for event venues or enterprise campuses) and slice replacement when a designated slice is congested or unavailable, seamlessly switching traffic to an alternative slice to guarantee user experience and slice reliability.

New revenue from analytics and exposure

Expansion of the 5G core network data analytics function (NWDAF) in Release 18 allows operators to monetize advanced network insights, especially for industrial IoT or VR content providers that require real-time traffic or QoS data. Collectively, Release 18 supports a range of open API enhancements turning the 5G-A core into a programmable platform that exposes time, QoS, slice, edge, and analytics capabilities in a way that external developers and enterprise systems can easily consume and monetize.

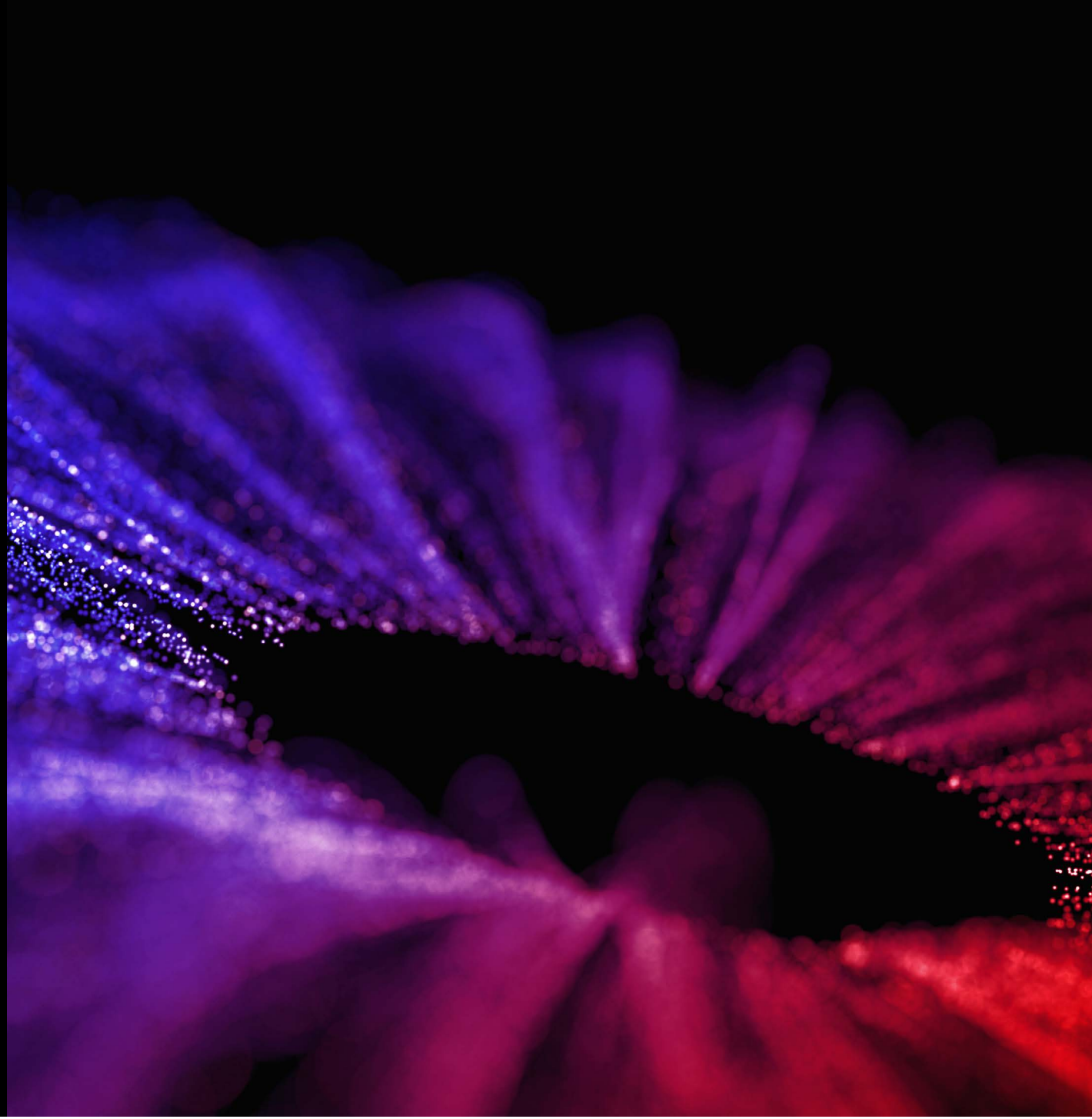
Release 18 turns the 5G-A core into a programmable platform that exposes time, QoS, slice, edge, and analytics capabilities in a way that external developers and enterprise systems can easily consume and monetize.

Energy efficiency and sustainability

Release 18 energy-efficiency additions provide operators a common way to measure, compare, and orchestrate power usage across RAN, core, and cloud infrastructures. Cell discontinuous transmission (DTX) and discontinuous reception (DRX), beam deactivation, and smarter channel state information (CSI) will give the largest kWh savings, while long device eDRX sleep modes turn 5G-A into a primary option for battery-powered IoT.

CHAPTER 3

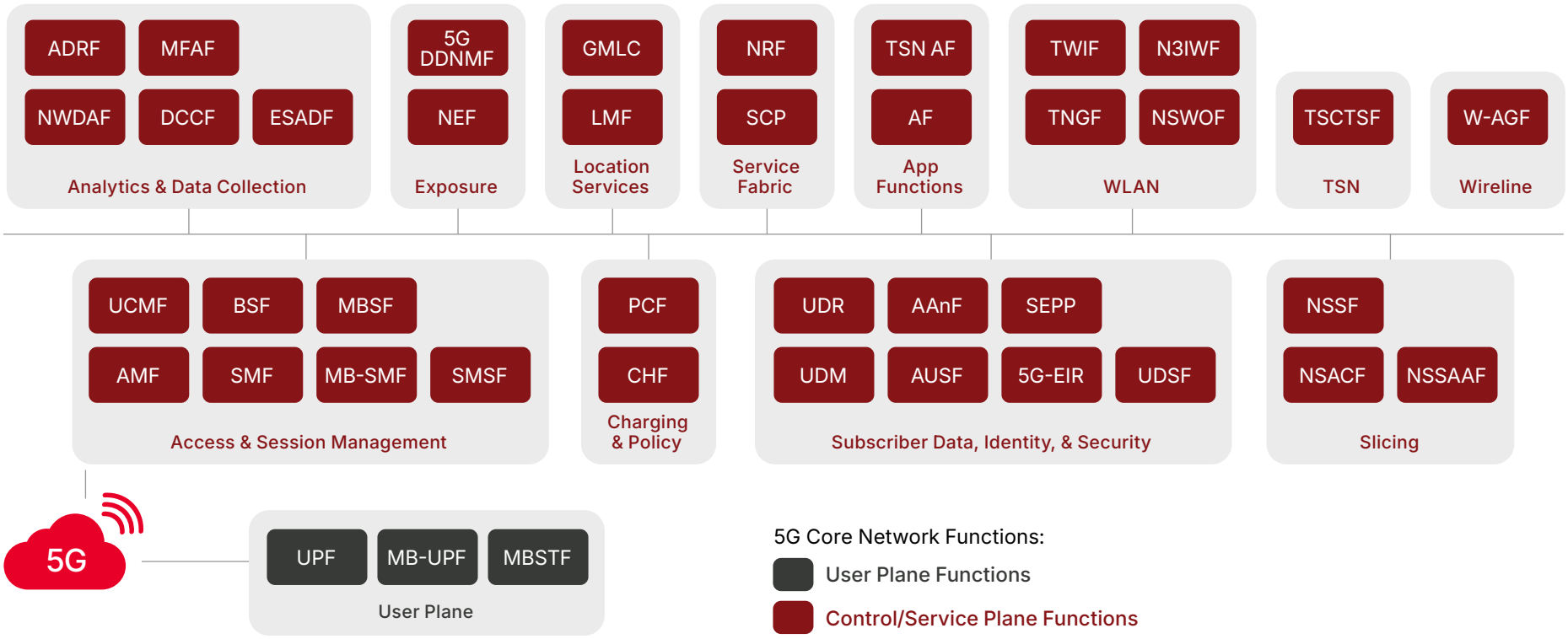
Why the 5G Core is Key to Creating 5G-A Value



CHAPTER 3

Why the 5G Core is Key to Creating 5G-A Value

The evolution of the 5G core is integral to the 5G-Advanced promise, serving as the control point for intelligent service delivery and coordinating everything from slice orchestration and policy enforcement to real-time analytics, edge offload, and exposure functions. In Release 18, the core becomes even more critical as operators move from baseline connectivity to differentiated, programmable services.



The high-level architecture diagram shows how the 5G core has expanded in Release 18 to support a broader set of functions across exposure, analytics, identity, location, and more.

While this architecture introduces greater flexibility for operators, the accompanying complexity requires more responsibility to validate that each element works as intended under real-world conditions.

Let's explore how the 5G core plays a central role in enabling key Release 18 features and why these areas demand focused validation and assurance.

Deeper slicing and policy control

Network slicing evolves in Release 18 to address varied consumer and enterprise demands. For example, the core enables partial slices, slice replacement, and slice capacity enforcement. 5G core, via functions such as session management function (SMF) and policy control function (PCF), is responsible for slice selection, policy enforcement, and end-to-end resource orchestration.

Multi-access and edge integration

5G-A fosters local breakout for edge computing, non-3GPP access (e.g., Wi-Fi or wireline), and access traffic steering, switching, and splitting (ATSSS). To support integration, the 5G core makes critical decisions about path selection, local data anchoring, roaming support, and analytics for next-level performance and reliability.

Support for complex vertical use cases

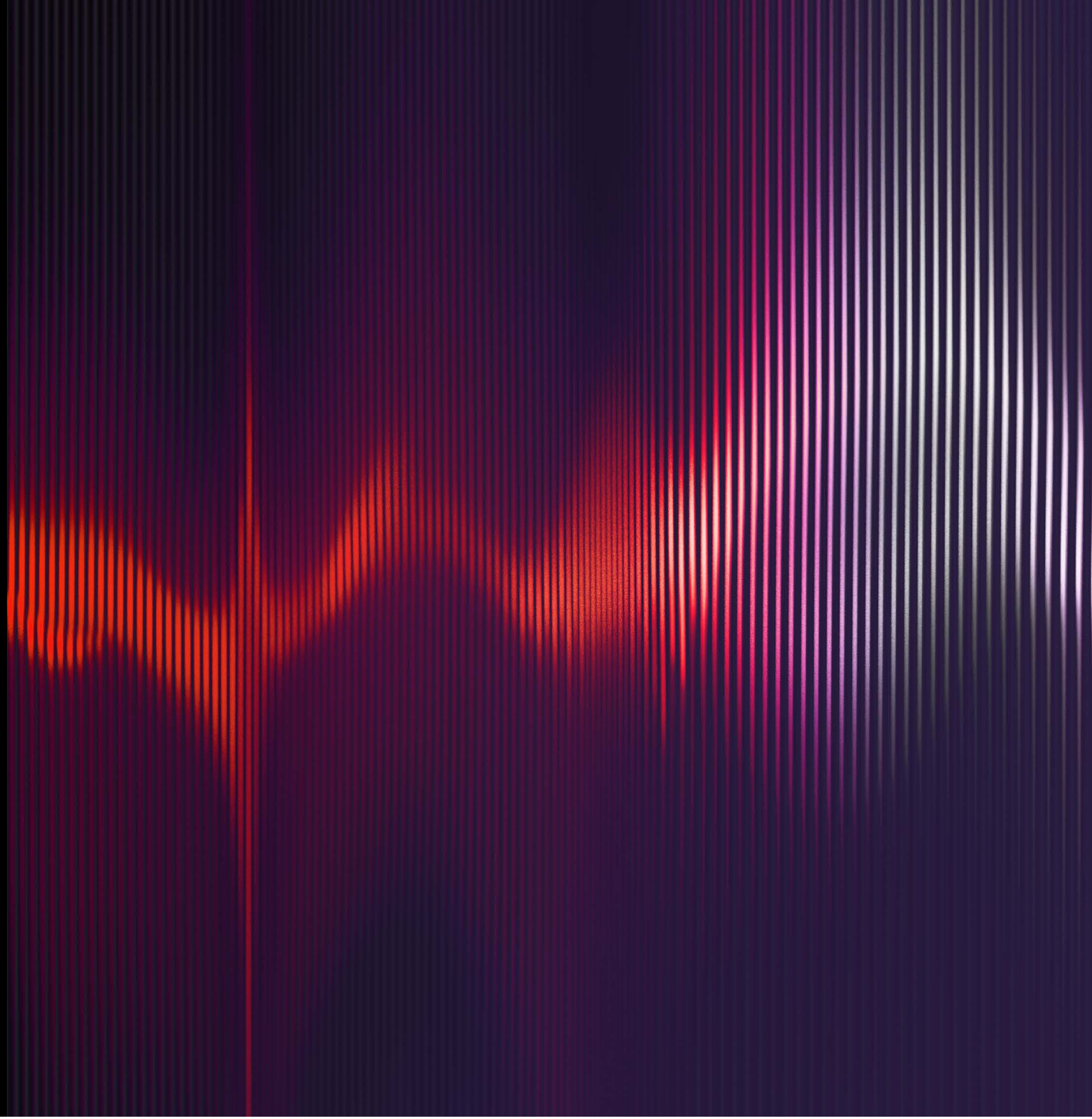
In 5G-A, UAVs, satellite integration, AR/VR, and mission-critical IoT all have distinct QoS, security, and subscription profiles. The 5G core manages these profiles, handling new interactions (e.g., for control plane and user plane event exposure), and ensures stable sessions across all RAN or edge topologies.

Exposure and monetization

Release 18 expands the 5G core exposure capabilities (network exposure function [NEF], NWDAF, network slicing), allowing operators to monetize advanced analytics and real-time policy from the core. The 5G core is critical for orchestrating slicing, dynamic QoS, and local breakouts, enabling new revenue opportunities and improved user experiences.

CHAPTER 4

Test and Assurance for Key Release 18 Features



CHAPTER 4

Test and Assurance for Key Release 18 Features

Non-terrestrial networks (NTN)

Release 18 enhances 5G support for satellite-based non-terrestrial networks, extending coverage, improving IoT performance, and ensuring service continuity during satellite transitions.

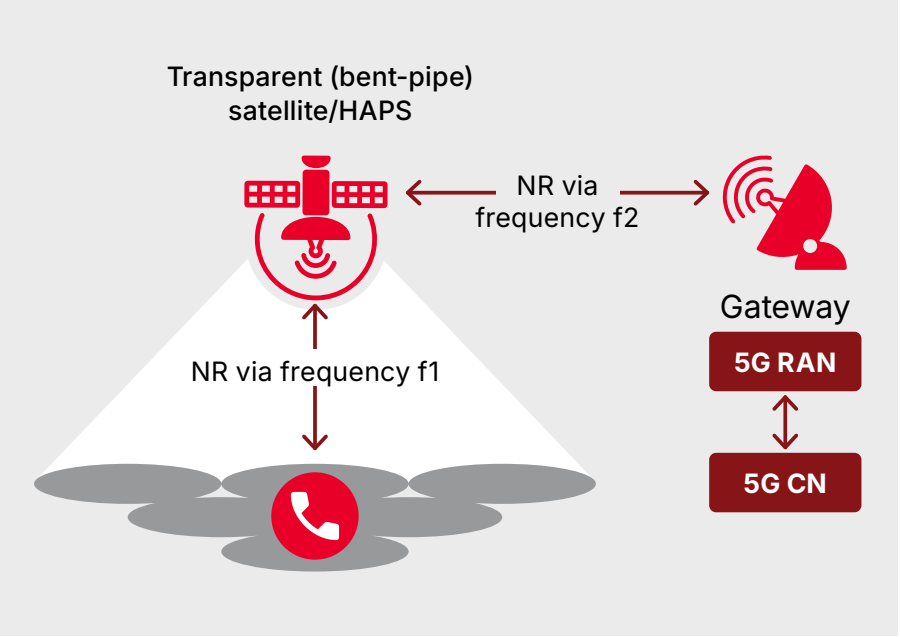
Release 18 capability overview

Discontinuous coverage handling lets devices sleep when out of range and efficiently reattach on the next satellite pass, with signaling overload controls to prevent attach storms when thousands of user equipment (UE) devices regain coverage simultaneously.

New satellite operating bands include support for L/S band (n254).

IoT-NTN enhancements improve data rates and mobility for battery-constrained IoT sensors served by satellites.

Mobility and handover refinements reduce random access congestion and minimize service interruption during satellite or beam switches.



5G core: impact and requirements

Release 18 updates the 5G core so it can understand where the satellite is in the end-to-end path, how its backhaul is behaving, and anchor the user plane directly onboard the satellite.

Satellite backhaul classification tags each NG-RAN node as geostationary Earth orbit (GEO), medium Earth orbit (MEO), and low Earth orbit (LEO), or other based on latency and bandwidth, with access and mobility management function (AMF) notifying SMF when the category changes to trigger QoS re-evaluation.

User plane breakout onboard satellites allows an edge user plane function (UPF) to sit on the satellite, enabling low-latency UE-to-UE traffic with a single satellite hop.

UE route selection policy (URSP) route descriptors for satellite slices let PCF insert satellite-specific rules so the UE requests the appropriate slice external data network name (DNN) or slice for application needs.

Satellite ID tracking during handovers ensures the AMF stores and passes current satellite ID to SMF and PCF, maintaining policy and routing continuity.

Core-triggered location verification supports lawful intercept and emergency services using a multi-round-trip time (multi-RTT) procedure that provides about 10 km accuracy with a single satellite in view.

Test and assurance considerations

Testing must ensure that the 5G core delivers Release 18's satellite-specific mobility, power-saving, and regulatory features without degrading user experience.

Large-scale UE reattachment testing should combine real handset over-the-air (OTA) testing with emulating thousands of UEs waking and reattaching to validate AMF throttling timers, randomization, and reject-with-timer behavior, ensuring high attach success and no excessive CPU load.

NTN<–>TN and TN<–>NTN session testing should run traffic sessions during handovers to measure interruption time, packet loss, and confirm AMF preserves protocol data unit (PDU) session and slice context.

Core buffering verification must confirm that AMF and SMF correctly buffer data while UEs are out of coverage and deliver it promptly upon reattachment.

Location accuracy and compliance testing should validate that core-triggered procedures correctly trigger UE location reporting for emergency response and lawful intercept.

Enhanced reduced capability (eRedCap)

Release 18 enhances the RedCap feature introduced in Release 17, further reducing device complexity and power consumption while improving coverage and latency. These updates broaden the 5G IoT device market and support use cases currently served by LTE Cat 1 and Cat 1 bis.

Release 18 capability overview

Reduced peak data rates cap uplink and downlink at 10 Mbps, enabling simpler hardware and lower power consumption.

Extended eDRX in RRC_INACTIVE supports long discontinuous reception cycles, allowing deep sleep modes while maintaining network connectivity.

5G core: impact and requirements

Release 18 introduces targeted 5G core enhancements to support power-efficient, low-complexity eRedCap devices with consistent policy enforcement, session handling, and data delivery tailored to constrained device behavior.

eRedCap-specific policy handling lets the core store and apply device-specific rules such as peak rate limits and extended inactivity timers.

Downlink data buffering for sleeping UEs ensures that the core holds data until the device wakes up, significantly reducing power draw.

	RedCap	eRedCap
Baseband bandwidth FR1	20 MHz	5 MHz and 20 MHz
Peak data rate FR1 (DL/UL)	220 Mbps / 120 Mbps	10 Mbps / 10 Mbps
Power saving	RRC idle state = up to about 3 hours RRC inactive state = up to 10.4 seconds	RRC idle state = up to about 3 hours RRC inactive state = up to 3 hours
Device complexity	Medium	Low
Battery life	Medium	Long
Cost	Low	Ultra-low

Test and assurance considerations

Testing must ensure that the 5G core delivers Release 18's eRedCap power saving, complexity reduction, and small data handling features without impacting user experience.

Peak rate compliance testing must validate that large data transfers never exceed the 10 Mbps ceiling.

Sleep-mode buffering validation should run traffic bursts while the UE sleeps to verify AMF and SMF buffering, paging behavior, and data delivery within the configured paging time window (PTW).

Latency and battery impact measurement should confirm downlink latency is within PTW and that battery draw is reduced as expected.

Comparative download time testing must measure eRedCap UE performance against full 5G NR UEs to ensure predictable and acceptable QoE.

Slice admission validation should confirm the AMF correctly handles slice assignment for eRedCap devices.

Extended reality (XR)

Release 18 elevates XR from a best-effort service to a tightly managed experience by enhancing scheduling, QoS control, and edge offload. These upgrades enable interactive XR with low latency, reduced device power drain, and operator-grade AR services.

Release 18 capability overview

Bursty traffic scheduling in 5G RAN improves uplink throughput and cuts headset battery usage by accurately timing XR traffic transmissions.

XR-specific QoS policy support in 5G core ensures consistent latency and responsiveness for interactive XR while enabling the network to protect other traffic flows.

Edge offload with discovery and negotiation supports remote rendering via edge servers, allowing lightweight devices to deliver high-fidelity graphics.

Operator-grade AR and immersive real-time communication (RTC) services support use cases like conversational AR and business-class XR video calls.

5G core: impact and requirements

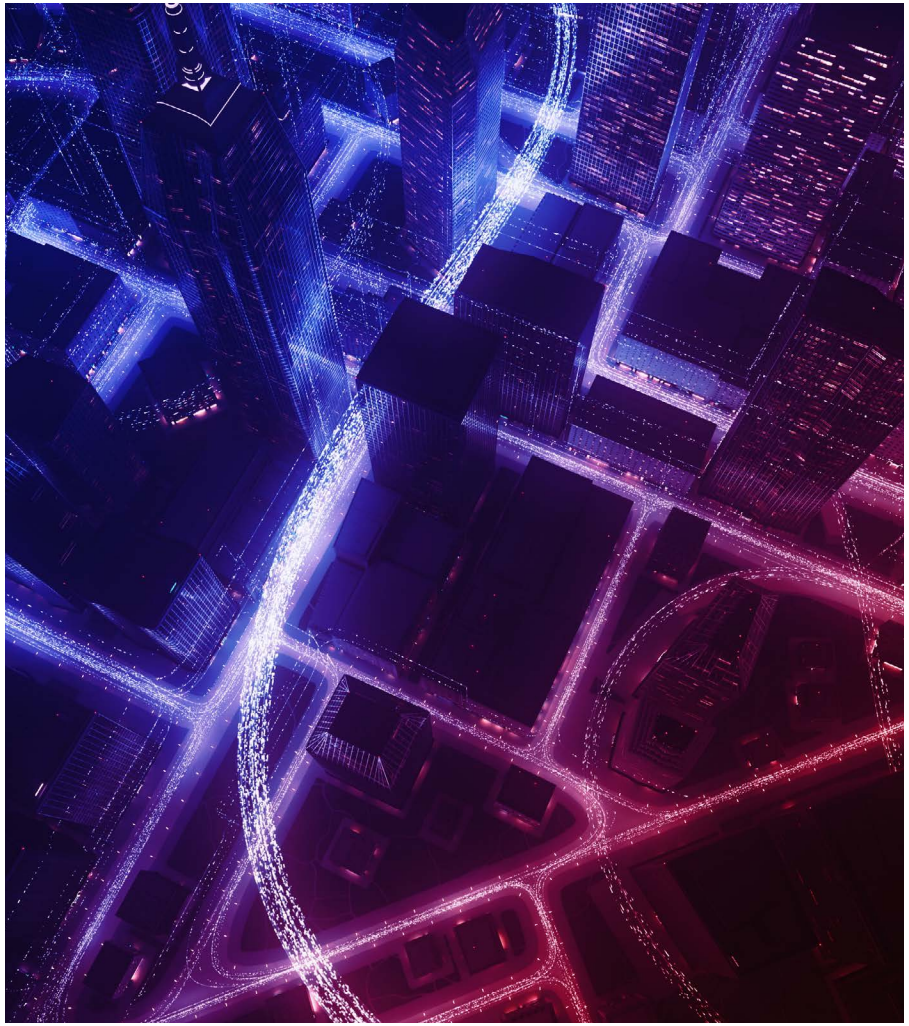
Release 18 adds fine-grained QoS control, real-time congestion exposure, and power-saving coordination so the 5G core can guide the RAN in prioritizing media streams and maintaining XR session quality.

Media unit prioritization for low-latency scheduling allows the UPF to forward XR frame importance tags to the NG-RAN, while PCF and SMF deliver PDU-set delay budget (PSDB) and error rate (PSER) indicators so RAN schedulers can minimize latency and drop non-critical frames under congestion.

Network-assisted power saving for XR lets the UPF signal data burst ends and jitter to help the RAN align DRX sleep windows with XR frame intervals.

Flow alignment across media types enables PCF to group parallel audio, video, and sensor flows into a shared “alignment group,” ensuring synchronized uplink and downlink scheduling to prevent playback drift.

Asymmetric QoS parameter support allows PCF to split uplink and downlink packet delay budgets (PDBs) and assign distinct 5QIs, which the SMF maps into bearer settings, giving RAN the flexibility to reserve more resources for heavier downlink traffic.



Test and assurance considerations

Testing must ensure the 5G core translates XR-specific Release 18 policies into predictable latency, adaptive behavior, seamless edge offload, and high-quality AR interactions.

PDU-set handling verification should inject streams with header extensions for PDU-set ID, importance (PSI), and end of data burst (EoDB), and confirm that the UPF passes metadata via GTP-U extension while NG-RAN correctly deprioritizes low-importance sets under congestion.

Latency budget validation must establish XR sessions requesting separate UL and DL PDBs and PSDB, confirming that configured values are enforced across the path.

Jitter and delay variation monitoring should stress test bursty uplink traffic and validate that SMF exports delay samples, PCF computes packet delay variation, and NEF/NWDAF distributes KPI updates.

Power savings confirmation should stream XR video and verify that the UPF's EoDB flag enables RAN to apply DRX cycles aligned with frame timing.

Edge computing (phase 2)

Release 18 enhances baseline edge computing capabilities by enabling roaming and inter-operator federation, allowing visited or partner edge clouds to securely host applications for home subscribers. New discovery, continuity, analytics, and security enhancements expand edge coverage across national, partner, and satellite domains.

Release 18 capability overview

Roaming and inter-operator federation support allows visited or partner edge networks to host applications for home UEs, enabling secure edge services across multiple footprints.

Extended discovery and continuity options help UEs locate common edge application servers (EAS) for group services, with support for handover to cloud, simultaneous connections to multiple EASs, and common API framework (CAPIF)-exposed APIs.

Application data analytics enablement (ADAE) provides real-time KPIs on edge load, slice performance, and application behavior to support predictive scaling, routing, or policy adjustments.

Satellite edge computing support enables selection of UPFs onboard satellites to support breakout and local switching.

Reinforced edge security applies per-entity authentication to control access to edge resources and breakout functions.

5G core: impact and requirements

Release 18 adds fine-grained QoS control, real-time congestion exposure, and power-saving coordination so the 5G core can guide the RAN in prioritizing media streams and maintaining XR session quality.

Federated edge path resolution uses new discovery data to let the AMF identify the appropriate distributed network access identifier (DNAI) and operator footprint, while the SMF anchors or re-anchors the PDU session to the selected UPF and maintains policy continuity as the UE moves across public land mobile network (PLMN) borders or shared edge sites.

Satellite UPF selection and local breakout lets the AMF provide satellite category and ID to the SMF, which selects a UPF onboard the satellite for local switching and breakout.

Real-time ADAE support allows ADAE services to collect edge load and application QoS metrics and feed predictions to applications or the PCF, enabling proactive resource and policy adjustments.

Edge-specific security enforcement enables NSSAAF, AMF, and PCF to issue and validate authorization tokens, rejecting unauthorized PDU session breakout requests.

Test and assurance considerations

Testing must ensure that the 5G core supports Release 18's new edge capabilities across roaming, federation, analytics, and security domains.

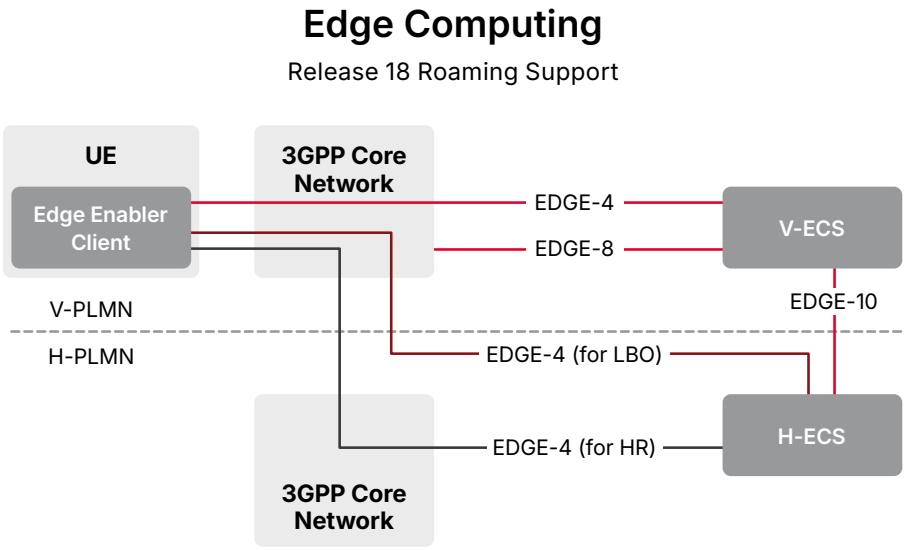
Roaming and federation validation should emulate UE attachment in visited and partner-edge environments to confirm AMF and SMF resolve the correct DNAI, establish local-breakout or home-routed sessions, and cleanly re-anchor as UEs cross PLMN borders.

Edge node sharing and re-anchoring must be validated by triggering on-demand edge instantiation and verifying that the SMF redirects traffic to the new EAS without data loss.

Satellite edge anchoring tests should confirm AMF sends satellite ID and category, SMF selects the onboard UPF, and UE-to-UE traffic is locally switched over a single satellite hop.

ADAE analytics performance should be tested by loading edge resources until thresholds are met and verifying that the ADAE server receives and exposes live edge load and application QoS KPIs.

Edge security testing must run full authentication flows and simulate unauthorized breakout attempts, confirming that NSSAAF and AMF block sessions lacking valid authorization.



Local Breakout (LBO) and Home Routed (HR)

Non-public networks (NPN) (phase 2)

Release 18 expands NPN capabilities to support seamless roaming between private networks operated by the same enterprise or its partners, while enabling secure access to standalone NPNs over trusted and untrusted non-3GPP connections. New support for localized services and tenant-specific visibility strengthens enterprise deployment and management options.

Release 18 capability overview

Seamless NPN roaming support allows devices to move between enterprise or partner-run private networks without repeating network selection.

Non-3GPP access to standalone NPNs (SNPNs) enables devices to connect over Wi-Fi or fixed broadband, using EAP-based mutual authentication and anonymous subscription concealed identifier (SUCI) for identity privacy.

Localized service support allows UEs to automatically attach to the nearest micro-NPN hosting a venue-specific application, such as on a factory floor or event site.

Tenant-aware network management provides enterprise customers with resource visibility, SLAs, fault KPIs, and access controls limited to their own slice of the shared public network.

5G core: impact and requirements

Release 18 upgrades the 5G core to support SNPNs and public network NPNs as full-mobility domains with secure authentication and localized service awareness.

SNPN-aware handover support enables the AMF to store and exchange SNPN lists during handovers so the target AMF can select the appropriate slice and policies without re-triggering network selection.

PDU session setup for SNPN access allows the SMF to accept SNPN identifiers over both 3GPP and non-3GPP access and apply localized service policies accordingly.

Expanded authentication methods support additional EAP types and anonymous SUCI formats in the AMF, unified data management (UDM), and security functions to enable secure access over untrusted Wi-Fi or broadband.

Local service-triggered traffic control allows the PCF and NEF to optionally prioritize or block traffic when UEs connect to localized services, enabling policy tuning for venue-specific behaviors.

Tenant-specific analytics and fault visibility let NWDAF filter KPIs, fault reports, and other data by NPN so enterprise users see only their network slice, even when using shared infrastructure.

Test and assurance considerations

Testing must ensure the 5G core reliably supports seamless mobility, secure multi-access, localized services, and tenant visibility for NPN phase 2.

SNPN mobility testing should combine real handset OTA testing with emulating UEs moving between two private networks while verifying that both AMFs maintain the PDU session and apply correct slice and policy settings without requiring re-selection.

Non-3GPP access and EAP validation should connect the same UE over trusted and untrusted Wi-Fi and fixed broadband, confirming authentication server function (AUSF) and AMF authentication, registration, and SMF session setup.

Localized service attach / leave testing must simulate UE entry and exit from coverage areas, validating automatic attach and resource allocation on entry and teardown on signal loss.

Tenant analytics testing should stream traffic and inject faults while confirming that NWDAF filters and exposes only the relevant KPIs and fault reports for the tenant's network slice.

Uncrewed aerial vehicles (UAVs)

Release 18 enhances UAV support by establishing a dedicated aircraft-to-anything (A2X) service layer and integrating altitude-aware mobility, policy-based flight management, and inter-operator coordination. These upgrades position 5G as a foundational platform for aviation-grade drone operations.

Release 18 capability overview

Dedicated A2X service layer provides drones with communication paths via PC5 sidelink and cellular, supporting broadcastremote ID (B-RID), low-latency command and control (C2), and detect and avoid (DAA) traffic.

A2X policy configuration via NEF allows operators or U-space managers to push spectrum, QoS, and security settings to UAVs through the 5G core.

Altitude-aware mobility and flightpath reporting adds support for subscription-based aerial-UE identifiers and enables the AMF to relay drone altitude and path data to gNBs for prioritization and interference control.

Multi-USS and dynamic airspace coordination supports seamless switching between U-space service suppliers (USSs) and allows area airspace managers (AAMs) to push no-fly zones and real-time UAV presence lists to drones and controllers.

5G core: impact and requirements

Release 18 adds aviation-grade capabilities to the 5G core to support policy, traffic management, and analytics for UAV operations.

UAV profile handling in AMF includes altitude limits, reporting permissions, and identifier flags, which are forwarded to serving and target gNBs during handovers for altitude-aware scheduling, while also enabling the AMF to authenticate drones attaching via PC5 sidelink without a traditional subscription.

Traffic class support in SMF, PCF, and UPF enables handling of specialized flows for B-RID, C2, and DAA, including unicast and multicast delivery.

Policy injection via NEF lets aviation and U-space systems push A2X policies and local steering commands for deployment in constrained environments such as stadiums.

Flight analytics from NWDAF exposes KPIs including altitude, congestion, sidelink usage, and message success rates to air traffic and safety systems.

Test and assurance considerations

Testing must confirm that Release 18 features support safe, policy-compliant, and latency-sensitive UAV operations in live airspace.

Altitude-aware mobility and QoS validation should confirm that the AMF forwards altitude events to SMF and PCF, triggers QoS or session release actions as required, and maintains active C2 and telemetry flows during handovers.

B-RID, C2, and DAA traffic handling tests should inject representative traffic types and verify that PCF applies the correct PCC rules, SMF anchors the sessions at the right UPF or MBMS gateway, and packet loss and latency stay within aviation requirements under load.

A2X policy enforcement validation must use NEF to push policy changes and confirm that AMF and SMF translate them into NGAP updates and that gNBs apply them correctly.

Analytics exposure tests should emulate UAV operations with B-RID and waypoint data and verify that NWDAF collects and exposes the expected counters and metrics.

Enhanced slicing (network slicing phase 3)

Release 18 upgrades slicing from a static configuration model to a dynamic, policy-driven framework with support for real-time availability, lifecycle control, and resource optimization across geographies, users, and time periods.

Release 18 capability overview

Time- and location-bound slicing allows operators to assign validity timers and partial location lists to slices, so UEs see only the slices available where and when they connect, even at the cell level.

On-demand slice usage policies let UEs register to a slice only when an application needs it and drop it after inactivity, reducing signaling load and improving spectrum efficiency.

Automatic slice replacement enables seamless switching to a pre-authorized alternative slice when the primary slice becomes congested or unavailable, with no user disruption.

Hierarchical quota enforcement and UE tracking introduces enhanced admission-control counters to monitor how many UEs already hold PDU sessions per slice, while operators can apply usage caps globally or regionally.

Per-slice EAP credentials via slice subscriber identity module (SSIM) allow devices to authenticate independently into multiple slices using credentials stored on as SSIM app.

5G core: impact and requirements

Release 18 transforms network slicing into a full lifecycle and policy management capability within the 5G core, enabling dynamic admission, enforcement, exposure, and authentication.

Per-slice validity and deregistration control in AMF store slice validity timers and push usage policy to UEs to trigger automatic deregistration and PDU session release.

Slice admission and switching in SMF and NSACF enable the SMF to handle PDU session moves during slice replacement and report slice usage; NSACF enforces quotas globally or per region.

Slice fallback logic in NSSF detects congestion or outages, selects alternative slices, and notifies the AMF to trigger the switch.

Policy enforcement in PCF applies slice usage rules, such as throttling on-demand slices when idle.

Slice telemetry exposure in NEF and NWDAF exposes real-time KPIs, diagnostics, and lifecycle operations to external consumers via the NSCE interface.

Slice exposure via network slice selection capability exposure (NSCE) APIs provides vertical customers and orchestrators with access to slice creation, diagnostics, KPI monitoring, and lifecycle management.

Test and assurance considerations

Testing must ensure the 5G core fully supports Release 18's dynamic slicing capabilities across lifecycle management, policy enforcement, and external exposure.

Slice validity and auto-deregistration tests should verify that UEs with slice usage policies correctly release slices after timers expire without affecting other PDU sessions.

Partial coverage mobility validation must simulate UE movement across cells where slice availability changes, confirming the AMF sends accurate availability lists and the device manages session drops or re-establishment gracefully.

Automatic slice replacement verification should inject congestion to trigger NSSF selection of an alternate S-NSSAI, with AMF and SMF switching sessions seamlessly and preserving QoS and data continuity.

Quota enforcement tests should load the network with concurrent registrations and PDU session requests to confirm network slice admission control function (NSACF) limits are applied when max UE thresholds are reached.

Slice exposure and telemetry testing must call NSCE and NEF APIs to create, query, and delete slices while running live traffic, and confirm consistency between exposed KPIs and NWDAF reports.

Mission critical and emergencies

Release 18 expands the mission-critical service suite (MCX) with new communication models, relay support, and direct device connectivity. These upgrades extend MCX capabilities to non-native devices and disconnected environments while strengthening security across all modes.

Release 18 capability overview

Ad-hoc group communication support allows authorized mission-critical push-to-talk (MCPTT), MCVideo, and MCData users to create temporary one-off groups for single-session use.

Gateway-UE relay model lets a smart radio device act as a proxy, routing MC signaling and media for nearby devices without MCX or universal integrated circuit card (UICC) capabilities.

MC services over 5G proximity services (ProSe) add support for both off-network direct communication and on-network UE-to-network relay, with administrator control over permitted traffic.

Mission-critical security phase 3 extends security coverage to all new MCX scenarios, including ad-hoc groups, relays, and off-network modes, across multiple domains and roaming contexts.

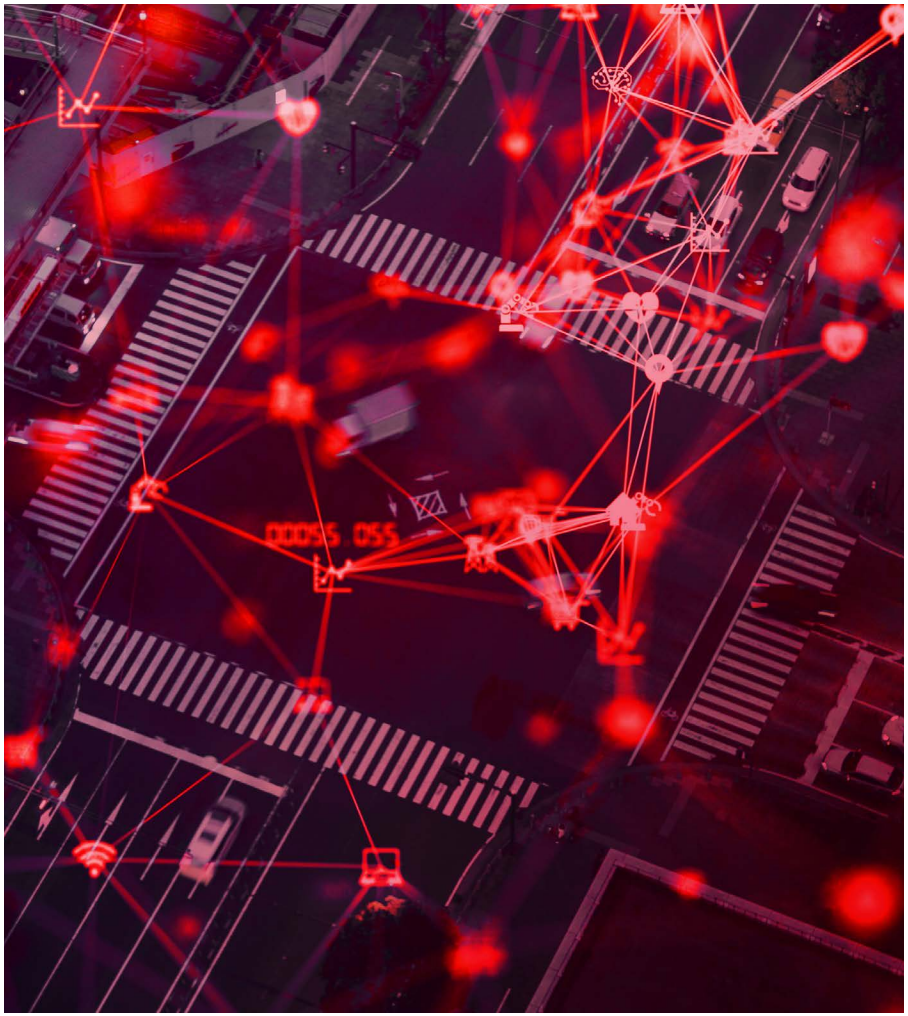
5G core: impact and requirements

Release 18 enhances 5G core functions to handle dynamic MCX sessions, proxy behavior, direct mode communication, and expanded security handling.

Ad-hoc group bearer management allows AMF, SMF, and PCF to recognize temporary MC sessions and apply dynamic QFI and QoS rules, re-anchoring bearers as participant lists change and ensuring continuity during handovers.

Relay flow handling for gateway UEs enables the AMF to flag proxied bearers, allowing the SMF to bind both the relay UE's IP flow and each proxied UE's multicast stream to a shared UPF and QoS profile, with the PCF enforcing per-relay traffic caps.

Group session support for 5G ProSe enables the 5G core to deliver group IDs, security parameters, and sidelink resource pool information to the UE for direct or relay communication modes.



Mission-critical key management in AUSF and UDM adds support for additional MC key epochs, securing access and message integrity in all MCX deployment contexts.

Test and assurance considerations

Testing must ensure that the 5G core and IMS properly support Release 18's new MCX service models, session control, relay behavior, and security extensions.

Ad-hoc group session lifecycle tests should emulate MC talk groups with participants joining and leaving while roaming, confirming that AMF triggers updates, SMF and PCF create and tear down temporary bearers, and handovers preserve active sessions.

Gateway-UE relay validation should simulate tethered device traffic through a proxy UE, confirming the core correctly flags relay flows, applies traffic caps, and maintains IMS features such as floor control and priority pre-emption.

5G ProSe path-switch testing should run group calls over MBS, force transitions to and from a 5G ProSe relay path, and verify seamless QoS mapping and audio/video continuity.

Mission-critical security checks should validate AUSF and UDM key management, including MC application server key handling and rejection of unauthorized devices.

Security and security assurance specification (SCAS)

Release 18 enhances the 5G security architecture with new capabilities addressing token scoping, certificate lifecycle, application-layer keying, and NPN over Wi-Fi, while introducing home-initiated authentication and consent-aware analytics. At the same time, SCAS is transformed into a complete, cloud-ready assurance framework covering all major 5G core, RAN, and management components.

Release 18 capability overview

Risk mitigation upgrades address architectural gaps in token scoping, certificate handling, NPN access over Wi-Fi, and app-layer keying, with added support for home-initiated authentication and consent-based analytics.

Comprehensive SCAS expansion now certifies 5G core functions such as PCF and authentication anchor function (AAnF), and extends to disaggregated gNB units (CU-CP, CU-UP, DU) with interface-level granularity (F1/E1).

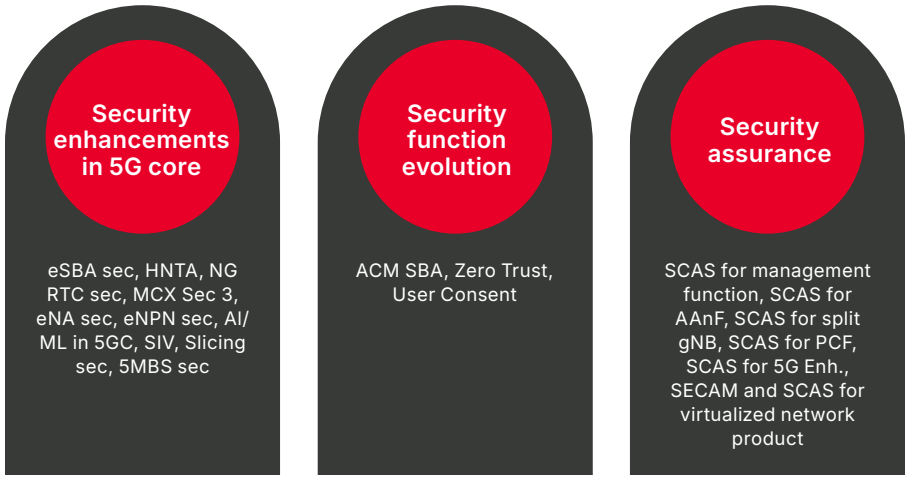
Cloud-native SCAS profiles introduce requirements tailored for containerized 3GPP functions, separating platform and function responsibilities.

SCAS requirement refresh aligns standards with EU5G and ENISA feedback, reinforcing SCAS as a recognized cybersecurity certification model.

5G core: impact and requirements

Release 18 strengthens 5G core security in authentication, service exposure, and cryptographic readiness.

Per-slice authentication via SSIM introduces a slice subscriber identity module that allows UEs to store unique EAP-TLS credentials per slice, with the AMF recognizing the SSIM flag, triggering separate NSSAA handshakes via AUSF/NSSAAF, and maintaining independent key hierarchies for each slice.



Zero Trust service exposure enforcement requires all service-based interfaces in the 5G core to use TLS 1.3 with mutual authentication and OAuth 2 token introspection before allowing NF-to-NF communication.

UPF traffic validation and logging mandates inspection of GTP-U extension headers and malformed SDAP PDUs, raising UP security breach alarms to the SMF and logging forensic metadata in the SCAS-defined format.

Crypto agility support introduces an algorithm negotiation framework allowing future re-keying with post-quantum or next-gen symmetric ciphers.

Test and assurance considerations

Testing must ensure that the 5G core and network functions comply with Release 18's enhanced security controls and SCAS certification framework.

SCAS compliance testing should execute the full Release 18 test suite for service-based interfaces, validating cipher suite negotiation, certificate validation, token introspection, replay protection, and compatibility with vendor and third-party public key infrastructures (PKIs).

SSIM and per-slice authentication tests must emulate simultaneous PDU sessions across multiple slices and verify that AMF and AUSF perform parallel NSSAA procedures, maintain isolated EAP key chains, and support clean revocation of one slice without affecting others.

Zero Trust perimeter validation should simulate rogue NF instances outside the trusted network and attempt service discovery or SBI interactions, confirming that NRF and NSSF enforce registration and access control restrictions.

5G core location services (phase 3)

Release 18 strengthens the 5G core location services framework with high-accuracy positioning support, deferred reporting for power-sensitive devices, and richer exposure and policy control. A new fused location function (FLF) enables more reliable fixes using multi-source data, exposed via NEF and CAPIF APIs.

Release 18 capability overview

Positioning reference unit (PRU) support introduces a new network entity that anchors centimeter-grade location fixes, with the AMF tracking which PRUs are in range of each gNB or satellite beam.

Deferred fix support for battery-constrained UEs lets the LMF retrieve previously collected measurements instead of starting new high-power sessions.

Secure user plane tunnel for LCS allows the LMF or UE to exchange LPP messages through a dedicated tunnel anchored by the SMF, with QoS applied by the UPF and access rules governed by the PCF.

Fused location function combines data from multiple sources to generate more accurate and reliable position estimates, with APIs exposing performance targets for accuracy and power consumption to external applications.

5G core: impact and requirements

Release 18 enhances several core NFs to support high-precision, power-aware, and flexible location capabilities.

PRU integration in AMF and LMF formalizes the PRU as a network function, with the AMF forwarding PRU association messages to the LMF and maintaining PRU reachability per cell or beam.

Battery-constrained UE handling allows the AMF to flag stored-location-available status, enabling the LMF to retrieve buffered data instead of triggering a new session.

User plane LCS tunnel setup supports secure low-latency tunnels for LPP traffic, with the SMF anchoring the path, the UPF applying delay-sensitive QoS, and the PCF authorizing usage based on policy.

Policy controls in PCF allow configuration of power budget and accuracy tradeoffs for location reporting.

Test and assurance considerations

Testing must ensure that the 5G core supports accurate, efficient, and policy-aware Release 18 location services.

PRU association validation should confirm that the AMF sends association events to the LMF and that the LMF correctly selects the relevant PRU when generating a location fix.

Deferred fix retrieval testing should emulate a battery-constrained UE with stored measurements, verifying that the AMF flags the condition and the LMF retrieves buffered data without triggering a new session.

User plane tunnel validation should establish a secure LPP tunnel via SMF and UPF, confirm PCF authorization, and verify that positioning messages meet RTT targets even under control plane congestion.

Location policy enforcement tests should apply a PCF rule linking accuracy targets to power budget constraints and confirm appropriate system behavior.

Railway communications

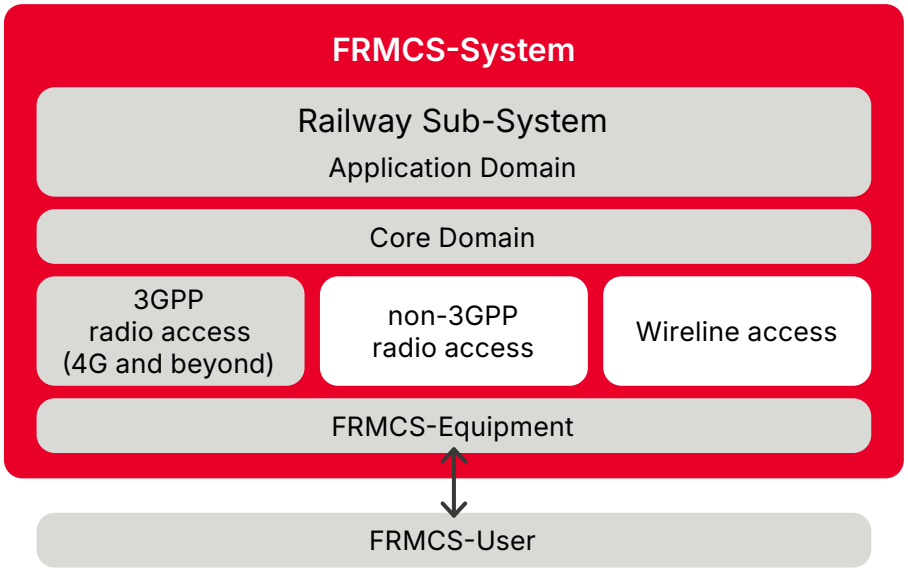
Release 18 introduces a railway-optimized air interface and spectrum profile to support the migration from Global System for Mobile Communications – Railway (GSM-R) to Future Railways Mobile Communication System (FRMCS), while enhancing 5G core capabilities to manage ultra-reliable control, onboard data backhaul, and passenger services over shared infrastructure. These upgrades allow national railways to transition to digital FRMCS systems without disrupting existing operations.

Release 18 capability overview

Railway-tailored air interface and spectrum profile supports a smooth migration from GSM-R to FRMCS, enabling reliable control signaling and broadband services over a single trackside network.

Multi-traffic core management supports concurrent ultra-reliable train control, high-throughput onboard CCTV, and best-effort passenger Wi-Fi, each with distinct QoS targets.

Stepwise migration and interconnection features help national operators phase in FRMCS without coverage gaps, ensuring continuity of mission-critical and passenger services during the transition.



5G core: impact and requirements

Release 18 enables the 5G core to deliver railway-aware performance through profiles, slicing, and policy enforcement aligned with FRMCS safety and service goals.

Rail-UE profile handling in AMF tracks train-specific identifiers, speed limits, and service priority, enabling paging and mobility support for UEs traveling at speeds ≥ 500 km/h. The AMF forwards priority data to the gNB during handovers.

Service-specific slice management in SMF creates URLLC slices for train control, high-throughput slices for CCTV/media, and best-effort slices for passenger services. SMF anchors control flows at trackside or edge UPFs and shifts large sessions to depot UPFs as trains stop.

QoS and priority mapping in PCF assigns rail traffic to distinct 5QI/QCI levels and ensures policies uphold deterministic performance for safety-critical control flows.

Per-flow policing in UPF enables gigabit-scale uplink bursts, local breakout for depot LAN offloads, and intra-train LAN switching for inter-carriage traffic.

Test and assurance considerations

Testing must verify that the 5G core supports high-speed mobility, deterministic control traffic, and flexible backhaul handling for FRMCS deployment.

High-speed mobility and URLLC continuity tests should combine real handset OTA testing with emulating train-mounted UEs moving across cells at ≥ 500 km/h, verifying seamless AMF and SMF handovers while preserving control slice KPIs.

Priority enforcement under traffic load should simulate heavy passenger and CCTV usage alongside injected deterministic control packets, confirming that PCF and SMF uphold rail traffic priorities.

Depot offload validation must confirm that large media uploads are successfully redirected to depot edge UPFs and meet required throughput guarantees.

Slice and quota enforcement tests should run concurrent sessions across URLLC, media, and Wi-Fi slices, verifying that SMF and PCF enforce quotas and that NWDAF analytics reflect real-time usage correctly.

Vehicle-to-everything (V2X)

Release 18 expands 5G V2X from a sidelink-only capability into a fully integrated, multi-bearer service managed end-to-end by the 5G core. These upgrades enable broadcast safety alerts, high-throughput sensor sharing, and centimeter-level relative positioning in a single cohesive V2X framework.

Release 18 capability overview

Multicast broadcast integration allows V2X application servers to push safety messages through 5G MBS, with end-to-end delivery managed by the core.

Sidelink evolution with core assistance enables the network to steer sidelink usage and adjust carrier assignment dynamically per QoS flow.

UE-to-UE relay under core control gives the SMF oversight of sidelink relaying, ensuring continuity and automatic fallback when link conditions change.

Network-assisted positioning introduces centimeter-grade sidelink ranging coordinated by the LMF, authorized by the AMF, and delivered over low-latency QoS bearers.

5G core: impact and requirements

Release 18 upgrades the 5G core to fully manage V2X as a network-coordinated service, with support for multicast, policy-controlled sidelink, relay supervision, and integrated positioning.

Multicast broadcast delivery support enables PCF, SMF, and UPF to route packets from V2X application servers to all UEs in a service area using MBS sessions.

Carrier steering for sidelink flows allows the core to direct which carriers a UE should use per flow and trigger carrier switching based on quality degradation.

Network-assisted sidelink positioning lets the AMF authorize ranging sessions, the LMF coordinate measurement exchanges, and the SMF and PCF allocate low-latency QoS for positioning data. NEF exposes APIs for external ITS platforms to initiate or subscribe to these sessions.

Relay anchoring and session continuity ensures that the SMF anchors UE-to-UE relay flows at the UPF and can automatically switch relay roles or revert to direct communication when the path recovers.

Test and assurance considerations

Testing must confirm the 5G core enables reliable safety message delivery, accurate positioning, and seamless session continuity for V2X services.

Multicast broadcast path validation should inject safety messages from a V2X application server, confirm MB-SMF session creation, and verify end-to-end latency meets road safety targets.

Network-assisted positioning validation must trigger a ranging request via NEF, confirm AMF authorization, LMF coordination, and timely delivery of the relative vector fix within the QoS flow.

Sidelink carrier handover testing should emulate dual-flow movement across cell borders, confirming AMF carrier map updates and uninterrupted session continuity from PCF and SMF.

Relay continuity validation should simulate UE-to-UE relaying, verify that the SMF anchors traffic at the UPF, and confirm the system automatically reverts when direct communication is restored.

CHAPTER 5

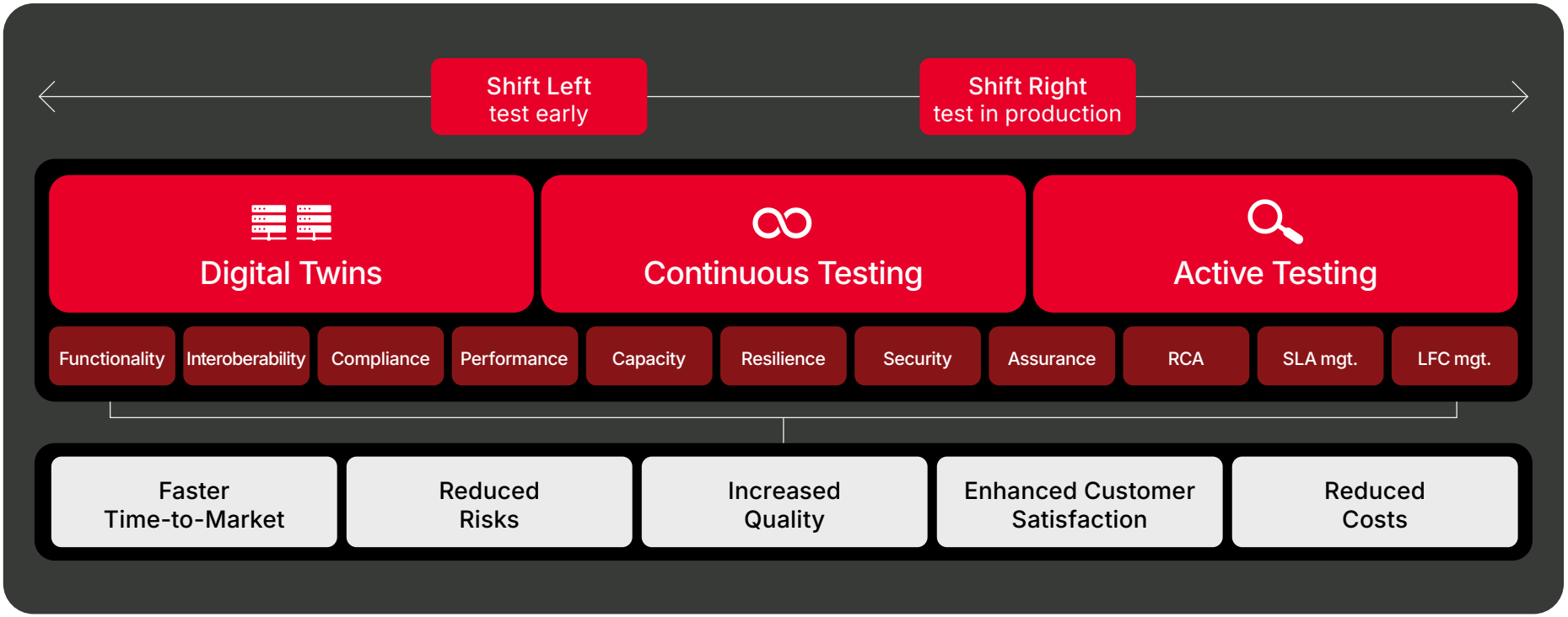
Test and Assurance for 5G-A Deployments

CHAPTER 4

Test and Assurance for 5G-A Deployments

5G-A introduces new functions, capabilities and a steady stream of updates that must be tested before deployment in the operational network. Tests range from traditional functional and interoperability testing to performance and security assessments.

The 5G-A testing lifecycle needs to be continuous, starting early to impact planning (shift testing left) and continuing into the production network (shift right) to ensure service quality.



Advanced methodologies such as digital twins, continuous testing, and active service assurance incorporate powerful, automated testing into the entire lab-to-live lifecycle to ensure any changes are thoroughly tested before being deployed.

Such comprehensive testing results in faster time-to-market, reduced risks and costs, and enhanced quality and customer satisfaction.

Digital twins using network and traffic emulators

Network and traffic emulators enable engineers to fully stress-test 5G-A features in a safe, controllable sandbox long before those features reach paying subscribers. The emulators effectively create digital twins of the 5G network that can be manipulated at will and do not require building out expensive test labs with 5G network equipment.

Emulators can spin up hundreds of thousands or millions of virtual eRedCap sensors, model intermittent NTN satellite coverage, replay bursty traffic across partial slices, and introduce chaos to truly validate resilience.

Because digital twins can also accurately emulate 5G core functions such as AMF, SMF, NWDAF, and PCF, operators can rapidly validate vendor performance, interoperability, compliance, security, and lifecycle management to assess behavior and responses under real-world, peak-load, and worst-case conditions.

The digital twin environment embeds automated security and 5G SCAS testing into the methodology so that every new feature, network function, or lifecycle update is validated against realistic scenarios.

Hybrid emulation and OTA testing for comprehensive validation

Combining digital twin emulation with over-the-air (OTA) testing using real handsets in the lab delivers the best of both worlds — controlled, repeatable end-to-end testing and realistic user experience validation.

This hybrid approach mirrors real subscriber behaviour across the device, RAN, and core, enabling complex scenario testing such as mobility, roaming, dual-SIM use, offload, and concurrent app use.

It also uncovers hard-to-detect performance issues, ensuring applications, OS, devices, and services perform reliably under real-world conditions before deployment.

> The emulators effectively create digital twins of the 5G network that can be manipulated at will and do not require building out expensive test labs with 5G network equipment.

Continuous testing (within a CI/CD pipeline process)

With 5G-Advanced functions being cloud-native micro-services and vendors pushing updates out on an IT release cadence, continuous testing integrated into a CI/CD pipeline is critical to turn every commit or change into an automated and seamless “validation exam” covering the complex plethora of testing, performance, conformance, interoperability, security, resilience, etc.

Pipeline triggered tests are spun up automatically to emulate network functions for wrap-around testing, and to generate synthetic traffic and impairments to provide realism. Defects that once surfaced weeks later in the lab, or worse, in production, are caught within minutes, keeping mean time to repair (MTTR) low and feature velocity high without sacrificing reliability.

Equally important, continuous testing underpins lifecycle management with the pipeline automatically re-running regression tests against the live canary instance, automating rollbacks if failures occur. This closed loop process provides the confidence operators need to release and monetize 5G-Advanced services while innovating at hyperscale-cloud speed.

> Active testing is the operational “contract enforcer” that translates Release 18’s technical potential into verifiable quality, customer trust, and new revenue.

Active testing (network and service assurance)

Active testing in the live operational network injects synthetic traffic from the device edge through the RAN, transport networks, 5G core, and out to real application servers, it has become indispensable in assuring the 5G era.

In 5G-Advanced, features such as partial-slice admission, ATSSS steering, eRedCap long-eDRX buffering, and satellite coverage re-entry only reveal their true behavior when the network is actively tested end-to-end under realistic traffic behaviors, latency, and mobility conditions.

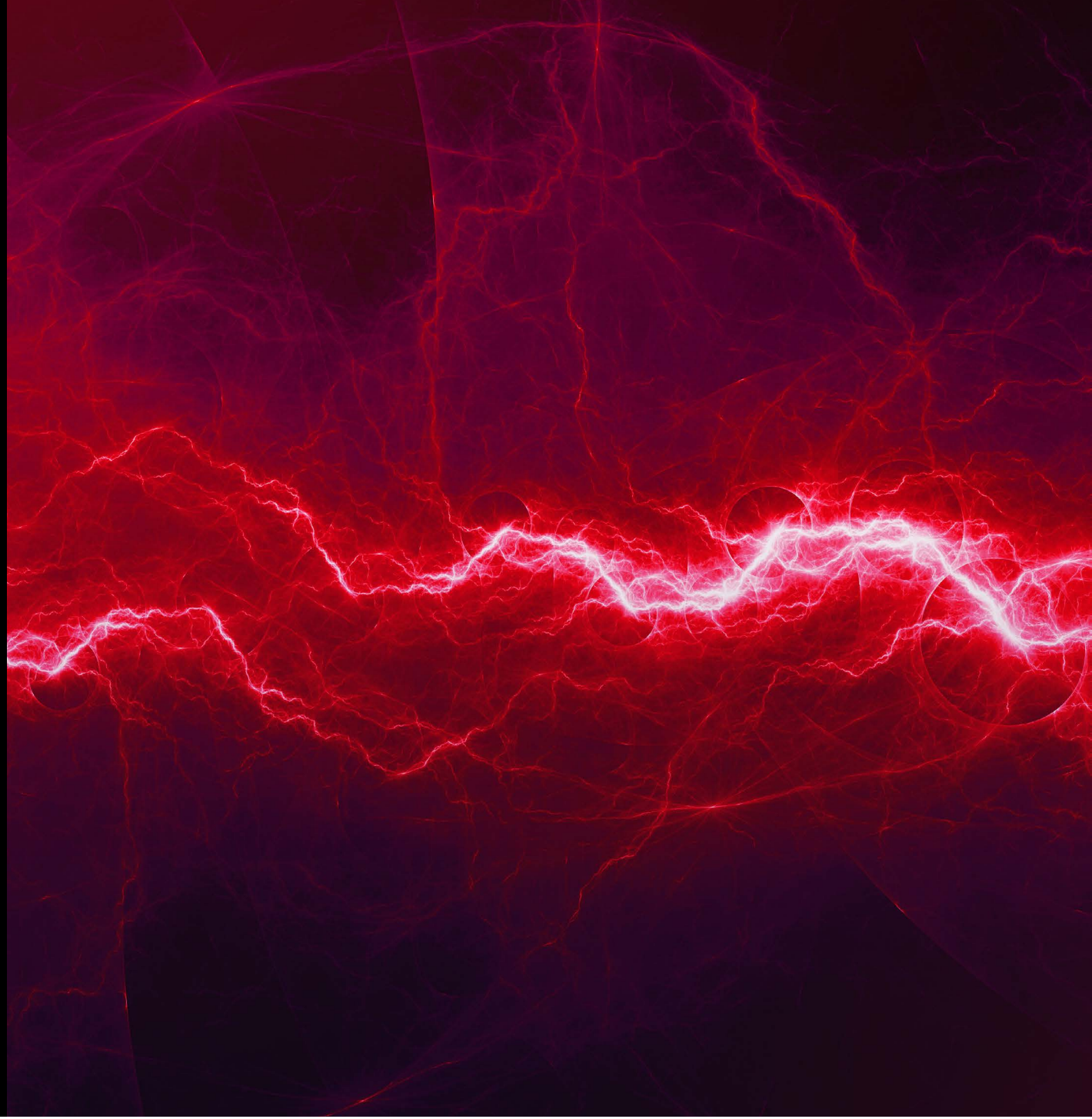
Operators can proactively expose hidden policy conflicts, anomalies, faults, or buffer-bloat long before paying customers experience degradations, outages, timeouts, or registration storms.

Active test agents also deliver a single source of truth (KPIs) giving engineering and business teams a single, objective proof of performance and a trustworthy set of service level agreements (SLAs) turning 5G-Advanced’s innovations into monetizable services.

Active testing provides evidence on demand, even as the network evolves with new software drops, configurations, or NF relocations. In short, active testing is the operational “contract enforcer” that translates Release 18’s technical potential into verifiable quality, customer trust, and, ultimately, new revenue streams for both consumer and enterprise markets. It has become table stakes for future AI development in the network.

CHAPTER 6

Conclusion and Takeaways



CHAPTER 6

Conclusion and Takeaways

Prepping 5G-Advanced strategies for business impact

Operators entering the 5G-Advanced era have a prime opportunity to supercharge monetization efforts across enterprise, industrial, and consumer markets.

But 5G SA is a necessary prerequisite to capitalize on the advanced core capabilities that comprise Release 18 as operators set sights beyond general connectivity improvements to support highly targeted, performance-driven services.

Importantly, stakeholders need not implement every 5G-A feature to begin reaping its value and vast benefits. The enhancements highlighted in this eBook serve as a practical guide to aligning capabilities against customized business goals, whether deploying private networks for manufacturing, launching XR experiences, or supporting railway and UAV operations. A phased approach supported by tailored adoption based on market demand can successfully expand a prosperous 5G-A strategy over time.

This evolution necessitates test and assurance strategies that shift from isolated moments in time to continuous, automated processes spanning the full network lifecycle.

Digital twins, CI/CD-integrated continuous testing, and active service assurance will play a central role in validating performance, detecting issues early, and proactively assuring that new features deliver anticipated outcomes. Embedding these methodologies into deployment and operations paves a path forward to confidently scale revenue-ready services across an array of 5G-Advanced use cases.

Keysight supports the 5G-A journey

As a market leader in 5G core network testing and assurance, Keysight works in close collaboration with leading operators and vendors to turn the 5G-Advanced promise into operational reality.

With deep expertise across 5G standalone, telecom cloud, lifecycle automation, and emerging Release 18 capabilities, Keysight supports end-to-end validation strategies tailored to changing network architectures. From the earliest phases of planning through continuous optimization, we are your trusted partner for confidently advancing toward high-value, differentiated services.

Keysight solutions span the full test and assurance lifecycle, from lab-based digital twins and CI/CD-integrated continuous testing to live, active service assurance in operational environments. Whether validating slicing logic, stress-testing satellite handovers, or assessing real-time quality of experience for XR or FWA services, Keysight's platforms and professional services can emulate, observe, and verify performance under real-world conditions. This approach ensures new features meet performance expectations, as well as commercial viability requirements.

5G-Advanced is driving new complexity in the network. Let us help simplify the path forward, providing the visibility and confidence to move faster, minimize risk, and unlock new growth opportunities. How can we help you turn the next era of 5G into measurable business impact?

LEARN MORE ABOUT KEYSIGHT'S SOLUTIONS →

Glossary of Acronyms

3GPP	3rd Generation Partnership Project
5G-A	5G-Advanced
5GC	5G core
5G-EIR	5G equipment identity register
5QI	5G QoS identifier
A2X	aircraft-to-anything
AAM	area airspace manager
AAnF	authentication anchor function
ACM	access control models
ADAE	application data analytics enablement
ADRF	analytics data repository function
AF	application function
AI/ML	artificial intelligence / machine learning
AMF	access and mobility management function
API	application programming interface
AR	augmented reality
ATSSS	access traffic steering, switching, and splitting
AUSF	authentication server function
B-RID	broadcast remote ID
BSF	binding support function
C2	command and control
CAPIF	common API framework
CCTV	closed-circuit television
CHF	charging function
CI/CD	continuous integration / continuous deployment
CN	core network
CPU	central processing unit
CSI	channel state information
CU-CP	centralized unit - control plane
CU-UP	centralized unit - user plane
DU	distributed unit
DAA	detect and avoid
DCCF	data collection coordination function
DDNMF	direct discovery name management function
DL/UL	downlink / uplink
DNAI	data network access identifier
DNN	data network name
DRX	discontinuous reception
DTX	discontinuous transmission
EAP	Extensible Authentication Protocol
EAS	edge application server
ECS	edge computing server
eDRX	extended DRX
EIR	equipment identity register
eMBB	enhanced mobile broadband
EoDS	end of data burst
eRedCap	enhanced reduced capability
ESADF	event streaming and data function
eSBA	enhanced service-based architecture
FLF	fused location function
FRMCS	Future Railway Mobile Communication System
FWA	fixed wireless access
GMLC	Gateway Mobile Location Center
gNB	next generation NodeB

GSM-R	Global System for Mobile Communications – Railway
GTP-U	GPRS tunneling protocol – user plane
H-PLMN	home public land mobile network
HAPS	high-altitude platform stations
HNTA	heterogeneous network traffic analysis
HR	home routed
IMS	IP multimedia subsystem
IoT	Internet of Things
IP	Internet Protocol
ITS	intelligent transportation systems
KPI	key performance indicator
LAN	local access network
LBO	local breakout
LCS	location services
LEO/MEO/GEO	low / medium / geostationary Earth orbit
LFC	local functionality control
LMF	location management function
LPP	LTE Positioning Protocol
MB-SMF	multicast broadcast – session management function
MB-UPF	multicast broadcast – user plane function
MBMS	multimedia broadcast / multicast service
MBS	multicast-broadcast services
MBSF	multicast broadcast service function
MBSTF	multicast broadcast session and transport function
MC	mission critical
MCPTT	mission-critical push-to-talk
MCX	mission-critical services
MFAF	messaging framework adapter function
MTC	machine-type communications
MTTR	mean time to repair
N3IWF	non-3GPP interworking function
NEF	network exposure function
NG	next generation
NGAP	next-generation application protocol
NPN	non-public networks
NR	new radio
NRF	network repository function
NSA	non-standalone
NSACF	network slice admission control function
NSCE	network slice selection capability exposure
NSSAA	network slice specific authentication and authorization
NSSAAF	network slice specific authentication and authorization function
NSSF	network slice selection function
NSWOF	network slice wireless orchestration function
NTN	non-terrestrial network
NWDAF	network data analytics function
PCC	policy and charging control
PCF	policy control function
PLMN	public land mobile network
ProSe	proximity services
PRU	positioning reference unit
PTW	paging time window
RCA	root cause analysis
RRC	radio resource control
RTT	round trip time
PDB	packet delay budget
PDU	protocol data unit
PKI	public key infrastructure
PSDB	PDU-set delay budget
PSER	PDU-set error rate
QFI	QoS flow identifier
QoE	quality of experience
QoS	quality of service
RAN	radio access network
RTC	real-time communication
SA	standalone
SBA	security behavior analysis
SBI	service-based interface
SCAS	security assurance specification
SCP	service communications protocol
SDAP	service data adaptation protocol
SECAM	security assurance methodology
SEPP	security edge protection proxy

SIV	synthetic intitialization vector
SLA	service level agreement
SMF	session management function
SMS	short message service
SMSF	short message service function
SNPN	standalone NPN
S-NSSAI	single network slice selection assistance information
SSIM	slice subscriber identity module
SUCI	subscription concealed identifier
TLS	transport layer security
TN	terrestrial network
TNGF	trusted non-3GPP gateway function
TSCTSF	time-sensitive communication translation and support function
TSN	time-sensitive networking
TSN AF	time-sensitive networking application function
TWIF	trusted WLAN interworking function
UAV	uncrewed aerial vehicle
UCMF	UE context management function
UDM	unified data management
UDR	unified data repository
UDSF	unstructured data storage function
UE	user equipment
UPF	user plane function
URLLC	ultra-reliable low latency communications
USS	U-space service suppliers
V2X	vehicle-to-everything
V-PLMN	visited public land mobile network
VR	virtual reality
W-AGF	wireline access gateway function
XR	extended reality
XR+M	extended reality + media

Keysight enables innovators to push the boundaries of engineering by quickly solving design, emulation, and test challenges to create the best product experiences. Start your innovation journey at www.keysight.com.