Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.1 2026 | Submission: 02/14/2026 | Accepted: 02/17/2026 | Publication: 02/20/2026

Cloud-native 5G core architectures

Cloud-native 5g core architectures

Native 5G core architectures in the cloud

Danyell Teixeira Soares is
a telecommunications engineer with 16 years of experience. He holds an MBA in Business Management from Fundação Getulio Vargas (FGV-SP, 2015) and a Bachelor's degree in Electrical Engineering with an emphasis in Telecommunications from the Pontifical Catholic University of São Paulo (PUC-SP, 2008).

Abstract: This article analyzes the technical and structural transformation of the mobile core in 5G Standalone (5G SA) networks , focusing on the transition from legacy elements to a Service-Based Architecture (SBA) and cloud-native functions (CNFs). It explains the interactions between AMF, SMF, UDM, AUSF, PCF, NRF, and UPF under the HTTP/2 protocol, orchestration via Kubernetes in stateless models, and security strategies oriented towards Zero Trust and Service Mesh. The study adopts as its methodology the analytical and documentary review of technical specifications of... 3GPP (Release 18), ETSI NFV recommendations, NIST standards, and international scientific literature. It is demonstrated that the operational resilience of the 5G core depends directly on real-time contextual observability, rigorous API contract management, and automated progressive validation mechanisms.

Keywords: 5G Core. Service-Based Architecture. CNF. Orchestration. Security APIs. Observability.

Abstract: This paper analyzes the technical and structural evolution of the mobile core in 5G Standalone (5G SA) networks, focusing on the transition from legacy elements to a Service-Based Architecture (SBA) and cloud-native network functions (CNFs). It details the interactions between AMF, SMF, UDM, AUSF, PCF, NRF, and UPF using HTTP/2, orchestration via Kubernetes in stateless models, and security strategies guided by Zero Trust and Service Mesh frameworks. The methodology is based on an analytical and documentary review of 3GPP Release 18 technical specifications, ETSI NFV recommendations, NIST standards, and peer-reviewed scientific literature. The findings show that the operational resilience of the 5G core directly relies on real-time contextual observability, strict API contract management, and automated progressive deployment validation.

Keywords: 5G Core. Service-Based Architecture. CNF. Orchestration. API Security. Observability.

1. Introduction

The consolidation of fifth-generation (5G) mobile networks represents a disruption. profound in relation to legacy telecommunications ecosystems, which historically They depended on rigid structures and proprietary, closed equipment. While the generations Previous solutions relied on dedicated nodes or structured first-generation virtualizations. Regarding bulky virtual machines (VNFs), the 5G Standalone (5G SA) specification It introduces a paradigm entirely focused on software, microservices, and native computing. in the cloud (KREUTZ et al., 2015; 3GPP, 2024a).

In this new architectural landscape, the 5G System (5GS) completely restructures the

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.1 2026 | Submission: 02/14/2026 | Accepted: 02/17/2026 | Publication: 02/20/2026

The control plane and the user plane are separated into decoupled components, called Functions.
Network Functions (NFs). Signaling between these functions is no longer performed.
via proprietary binary protocols over point-to-point links and adopts the model of
Service-Based Architecture (SBA), supported by
RESTful application programming interfaces (APIs) running over the HTTP/2 protocol
and data serialized in JSON (3GPP, 2024c).

This transition provides extraordinary gains in horizontal scalability.
Agility in deploying new features and optimizing the use of physical infrastructure.
Underlying: The ability to deploy and update network functions within short timeframes.
It transforms the dynamics of operators, allowing alignment with agile methodologies.
Continuous Integration and Development (CI/CD) are commonly observed in the technology sector.
of the information.

However, the migration to Cloud-Native Network Functions
Functions (CNFs) introduces unprecedented operational complexities for engineering teams.
Networking. The fragmentation of the control plane across hundreds of containers and microservices.
Dynamic technologies require highly sophisticated automated orchestration and discovery mechanisms.
service dynamics, continuous layered security management, and in-depth observability.
(BONDAN et al., 2016; YILMA et al., 2019).

Interoperability in environments composed of multiple vendors (compliance)
Technically, the theoretical benefits of service-oriented architecture can be negated by...
unpredictable operational instabilities.

The aim of this article is to thoroughly examine the internal architecture of the 5G Core.
(5GC), mapping the functional dynamics of NFs, the transition from VNFs to CNFs, the cycle of
The life of orchestration in Kubernetes, Zero Trust/Service Mesh security models, and the
observability requirements. The work is based strictly on the scientific literature.
peer-reviewed and in accordance with current 3GPP technical standards, offering a technical analysis.
Consistent, thorough, and fully traceable.

2 Methodology

To ensure the technical rigor and academic traceability of the analyses presented,
This research adopts as its method the analytical and systematic review of technical literature and
normative. The survey of the documentary corpus was restricted to primary and secondary sources.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.1 2026 | Submission: 02/14/2026 | Accepted: 02/17/2026 | Publication: 02/20/2026

with high institutional and academic recognition, organized to fully cover the The complexity of cloud-native mobile networks.

The first methodological axis comprises international normative specifications. The 3GPP (3rd Generation Partnership Project) relevant to Release 18 were analyzed. detailed documents TS 23.501 (system architecture), TS 23.502 (procedures) of the system), TS 29.500 (technical implementation by SBA) and TS 33.501 (security architecture). Additionally, the ETSI virtualization frameworks (GS NFV 002) were incorporated for to provide a basis for the analysis of the infrastructure layer.

The second axis encompasses the official guidelines of regulatory bodies and cybersecurity, including recommendations from NIST (National Institute of Standards and Technology - SP 800-204A) relating to the security of microservices-based applications and Service Mesh, in addition to the statistical data and global coverage reports published by International Telecommunication Union (ITU).

The third axis is based on the selection of peer-reviewed scientific articles and indexed in high-impact databases (IEEE Xplore, ScienceDirect/Elsevier and ACM Digital) (Library). The screening of these publications was based on direct verification of the Digital Object. Identifier (DOI), prioritizing empirical and conceptual studies focused on SDN, NFV, Container orchestration and mobile network security.

The synthesis of the information was based on an analytical matrix structured in five parts. Functional dimensions: definition of architectural roles, transport dependencies, modes of Failure in microservices, automated control mechanisms, and performance evidence. This framing avoided the inclusion of generic or speculative statements that did not that had direct support in the technical documentation analyzed.

Finally, all the material was structured and formatted in strict accordance with the ABNT standards for scientific writing. Bibliographic references have been standardized. According to NBR 6023, citations in the text follow NBR 10520, and the presentation of tables... The illustrations meet the formal criteria for legibility, numbering, and source indication.

3 Service-Based Architecture (SBA) and Functional Decomposition

The 5G Core architecture is based on the principle of strict separation between the plane. of control and the user plane (Control and User Plane Separation - CUPS). This premise ensures that the processing of access signaling and the transport of data traffic from

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.1 2026 | Submission: 02/14/2026 | Accepted: 02/17/2026 | Publication: 02/20/2026

subscribers can operate within completely independent computational structures, allowing that each layer scales in a customized and efficient way (3GPP, 2024a).

In the control plan, the central element of innovation is the consolidation of the Architecture. Service-Based Approach (SBA). In this approach, network functions (NFs) no longer communicate through pre-configured direct connections and begin to act as both consumers and providers of Services in an open communication network. Communication occurs on the bus. Services (Service-Based Interface - SBI), using the HTTP/2 protocol over TLS 1.3, with Payloads formatted in JSON (3GPP, 2024c).

Among the main NFs of the SBA, the AMF (Access and Mobility Management) stands out. Function), responsible for access control and mobility; the SMF (Session Management) Function), responsible for managing PDU data sessions; the UDM (Unified Data Management) Management), which centralizes subscriber profiles; the AUSF (Authentication Server) The Function), which executes the authentication algorithms; the PCF (Policy Control Function), which governs QoS rules and pricing; and the NRF (Network Repository Function), which acts as the central repository for dynamic service discovery (3GPP, 2024a).

Figura 1 – Desacoplamento Funcional e Arquitetura SBA do 5G Core

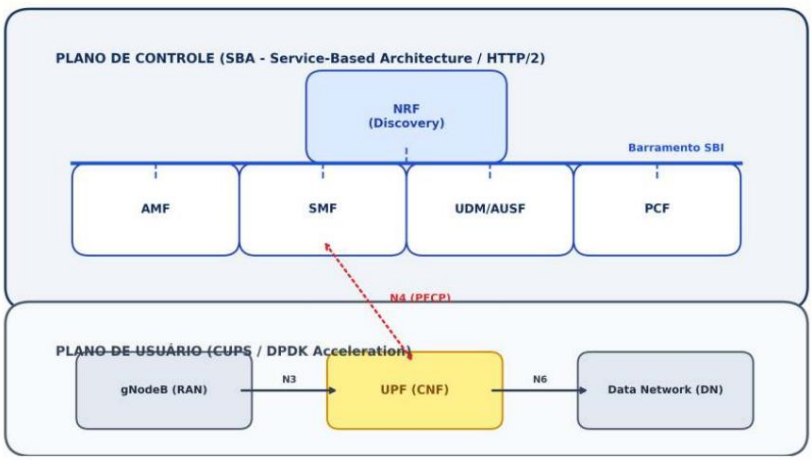

Figure 1 – Functional Decoupling and SBA Architecture of the 5G Core.
Source: Prepared based on 3GPP TS 23.501 (2024).

The operational dynamics of the SBA are coordinated directly by the NRF. When An instance of AMF or SMF is initialized in the cloud, and it performs its self-registration with the...

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.1 2026 | Submission: 02/14/2026 | Accepted: 02/17/2026 | Publication: 02/20/2026

NRF, stating its capabilities, location, and service profile. When another NF
If a specific service needs to be consumed, it queries the NRF to obtain the address and endpoint.
Updated versions of the desired function, eliminating the need for rigid static addressing.
(3GPP, 2024b).

At the user level, the only function responsible for packet transport is the UPF.
(User Plane Function). The UPF is remotely controlled by the SMF via the PFCP protocol.
(Packet Forwarding Control Protocol) on the N4 interface. This separation allows for the deployment of
UPF instances extremely close to the end user (Edge Computing), reducing
drastically reduce application latency while control remains centralized (3GPP,
2024a).

Another crucial advancement in SBA is the stateless model. Unlike the MME
and S-GW of 4G networks, which stored session states in local memory, the NFs of
5G SA offloads all user state and context into a database layer.
distributed and designated UDR (Unified Data Repository). This separation ensures that, if a
If an AMF or SMF instance fails, another identical instance can take over the service.
immediately, without interrupting users' active connections (KREUTZ et al., 2015).

4. Function Virtualization and the Transition from VNF to CNF

The evolution of 5G mobile infrastructure involved the gradual transition of hardware.
dedicated (*appliances*) for the Virtualized Network Functions (VNFs) model and,
later, to Cloud-Native Network Functions (CNFs). This trajectory reflects the pursuit
The sector's continuous pursuit of greater efficiency in the use of computing resources and modularity.
Code and speed of deployment (ETSI, 2014; NIST, 2020).

Virtual Network Interfaces (VNFs) represented the first step in this transformation by abstracting the hardware.
Physical systems are managed through hypervisors. However, VNFs bring the structural burden of requiring a system...
A complete guest operating system (Guest OS) for each virtual machine. This feature
results in high RAM consumption, slow boot times (in the range of
minutes) and tight coupling with infrastructure orchestration platforms (NIST, 2020).

CNFs, in turn, represent the native application of container concepts and
microservices are integrated into telecommunications networks. By sharing the same kernel as
On the host operating system, containers package only the application and its components.
Direct dependencies. This drastically reduces memory demand and allows for initialization.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.1 2026 | Submission: 02/14/2026 | Accepted: 02/17/2026 | Publication: 02/20/2026

in milliseconds and enables an incomparably higher deployment density in same physical server (BONDAN et al., 2016).

CNF architecture is the ideal foundation for supporting SBA granularity in 5G Core. Functions such as AMF or SMF cease to be monolithic blocks and are instead decomposed into... multiple independent microservices (e.g., authentication microservice, microservice of Mobility, microservice billing). Each microservice runs in its own container and It can be updated individually without affecting other parts of the network.

For the User Plan (UPF), which handles massive traffic on the order of gigabits or With terabits per second, the migration to containers required innovations in bypassing the kernel of Linux. The integration of technologies such as DPDK (Data Plane Development Kit) and SR-IOV. (Single Root I/O Virtualization) allows the UPF container to directly access the boards. of physical network interfaces (NICs), achieving line-speed forwarding rates with low latency. sub-milliseconds (BONDAN et al., 2016).

However, the adoption of CNFs imposes stringent requirements regarding safety isolation. and dependency management. Unlike virtual machines, which offer strong isolation. Based on hardware via a hypervisor, containers depend on logical kernel resources. Linux (namespaces and cgroups). Consequently, the infrastructure must be rigorously... Shielded to prevent vulnerabilities in the container from allowing evasion to the host node. (NIST, 2020).

5. Lifecycle Orchestration and Automation

The presence of hundreds of microservices distributed across containers makes management easier. A 5G Core manual is unfeasible. The orchestration and automation of the CNF lifecycle make- Therefore, they are mandatory components of the architecture. The market standard adopted for this The purpose is the Kubernetes (K8s) platform, operating in sync with the framework of ETSI NFV MANO (Management and Orchestration) orchestration (ETSI, 2014; YILMA et al., 2019).

Cloud-native automation relies on the declarative reconciliation model. Instead of executing imperative configuration commands, engineers define the state. The desired system output is determined through manifest files in YAML or JSON format. The orchestrator It continuously compares the actual state of the infrastructure with the desired state and executes automatically take the necessary actions to correct any discrepancies (YILMA et al.,

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.1 2026 | Submission: 02/14/2026 | Accepted: 02/17/2026 | Publication: 02/20/2026

2019).

In the context of Kubernetes, the management of complex CNFs is made possible by... Operator Pattern design pattern. An Operator is a custom controller that extends the The Kubernetes API is implemented through Custom Resource Definitions (CRDs). Operational knowledge of network functions, automating advanced tasks such as routines of Database backup, coordinated dependency initialization, and schema updates. Banking at UDR.

Automatic capacity scaling is another key benefit of orchestration. Using the Horizontal Pod Autoscaler (HPA), Kubernetes monitors metrics in real time. such as requests per second (RPS) rate in SBI or CPU usage in instances of AMF and SMF. When cargo exceeds established limits, new container replicas are used. They are created automatically in seconds to absorb peak traffic.

To ensure continuous updates without service interruption (zero downtime), Modern deployment strategies are used, such as Canary Deployments and Blue-Green Deployments. Deployments. A new version of the microservice is deployed in parallel with the current version; the The orchestrator redirects a small percentage of the traffic to the new version and monitors it. the error indicators. If the behavior is validated, the traffic is migrated in its entirety and The old version is deactivated.

However, automation in telecommunications networks requires special attention to... Hardware determinism. Packet processing loads on the UPF do not tolerate latency. A variable generated by unpredictable context switches in the CPU. For this reason, the orchestrator Kubernetes should be configured with advanced node affinity features (NUMA). awareness), processing core isolation (CPU pinning), and memory allocation of large page (*HugePages*) (YILMA et al., 2019).

6. API Security and Trust Between Microservices

The adoption of open interfaces based on HTTP/2 and REST in the Architecture Based In Services, it considerably expands the attack surface of 5G Core compared to Legacy networks. To protect the infrastructure against unauthorized access and tampering. lateral threat analysis, the 3GPP TS 33.501 and the NIST SP 800-204A standard establish the mandatory Zero Trust security model (NIST, 2020; 3GPP, 2024d).

In the Zero Trust model, no network function or microservice is considered.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.1 2026 | Submission: 02/14/2026 | Accepted: 02/17/2026 | Publication: 02/20/2026

Reliable by default, even when running within the perimeter of the internal network of operator. Any and all API requests transmitted on the service bus (SBI) must to be rigorously authenticated, authorized, and encrypted before being processed by the destination node. (NIST, 2020).

The first layer of protection in SBI is mutual authentication and encryption at the layer of Transport via TLS 1.3 (mTLS). Unlike traditional TLS, where only the server... It presents a digital certificate; mTLS requires that both the consumer invoice and the invoice... Providers must present valid x.509 certificates issued by a Key Infrastructure. Public (PKI) privately maintained by the operator (3GPP, 2024c).

The second layer of security operates at the application level through the OAuth protocol. 2.0. Simply validating the mTLS certificate establishes a secure channel, but does not guarantee security. Data access permission. To consume a service, the requesting NF must request a A JSON Web Token (JWT) access token is provided to the NRF. The NF provider validates the signature. The JWT digital token verifies if the permissions contained in the token authorize the execution of the call. specific (3GPP, 2024c).

To avoid developers having to implement the complex logic of mTLS and OAuth 2.0 token validation directly in the source code of each microservice. The Service Mesh architecture is used. In this approach, lightweight proxies are employed. (like the Envoy) are deployed as auxiliary containers (*sidecars*) alongside each NF container.

The *sidecar* proxy transparently intercepts all incoming and outgoing traffic from network function, managing the establishment of mTLS tunnels, management of digital certificates and workload identity validation (using standards such as SPIFFE/SPIRE). This ensures that security policies remain uniform across the board. mesh, regardless of the NF supplier (NIST, 2020).

7. Observability, Performance, and Reliability

In a highly distributed and dynamic ecosystem like native 5G Core in cloud, traditional infrastructure metrics (such as CPU usage percentage or occupancy) (disk) are completely insufficient to diagnose service failures. The warranty of Reliability and high availability require the implementation of an observability architecture. based on three fundamental pillars: metrics, distributed tracking, and event logs

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.1 2026 | Submission: 02/14/2026 | Accepted: 02/17/2026 | Publication: 02/20/2026

(BARAKABITZE et al., 2020).

The first pillar, focused on aggregated numerical metrics, uses time series collectors. Temporal systems (such as Prometheus) for monitoring Service Level Indicators (SLIs) and Key Performance Indicators (KPIs). In 5G networks, the most critical metrics include... success rate of user registrations in AMF, response time for establishing PDU sessions and the packet discard rate at UPF.

To gain an accurate view of the user experience, latency analysis in API calls in SBI should focus on percentile statistics, such as the 99th Percentile (P99). Measuring only average latency is misleading, as isolated delay spikes affecting 1% of the data can occur. Transactions may be hidden within seemingly normal averages, leading to glitches. Intermittent signaling in high load scenarios (BARAKABITZE et al., 2020).

The second pillar is distributed tracing. Like a single A request from a terminal (e.g., creating a data session) triggers a sequence. The complex API call system between AMF, SMF, UDM, PCF, and UPF makes it necessary correlate all these steps. The W3C Trace Context specification is used, injecting a A header containing a unique identifier (*Correlation-ID*) in the initial request.

The *Correlation-ID* is passed sequentially through all microservices. involved in the transaction. Visualization tools (such as Jaeger or Zipkin) utilize this identifier to draw the complete flow map, displaying the exact time spent at each point. microservice. This capability allows network engineering teams to identify With surgical precision, identify the specific function that introduced undue latency or caused a failure. processing.

The third pillar comprises event logs structured in a format... JSON. The logs provide detailed context of the failure when an error occurs, displaying Exception messages and application-specific error codes. Centralized consolidation Logging into real-time analytics platforms ensures post-audit capability. incident and support for preventative diagnoses underpinned by operational intelligence. (BARAKABITZE et al., 2020).

8 Migration, Interoperability and Validation

The transition from legacy 4G EPC (Evolved Packet Core) mobile networks to the architecture. 5G Core Standalone does not occur through an abrupt infrastructure replacement (*big-

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.1 2026 | Submission: 02/14/2026 | Accepted: 02/17/2026 | Publication: 02/20/2026

The financial cost and operational risk necessitate a gradual migration strategy and highly planned, ensuring the complete continuity of services provided to subscribers (ORDOÑEZ-LUCENA et al., 2017).

The first phase of this transition relies on the 5G Non-Standalone model (5G NSA - Option 3x). In this topology, the 5G radio network (gNodeB) is deployed as a layer. complementary capacity, but all control signaling and management of User mobility remains anchored in the legacy 4G EPC core infrastructure. through the MME node.

The second phase comprises the parallel deployment of 5G Core Standalone and the Establishing mechanisms for coexistence and interworking. Interoperability between The 4G core and the 5G core are maintained through the N26 interface, which directly interconnects the MME to AMF. This interface allows for transparent handovers and... Continuity of data session when a mobile user moves between 4G and 5G coverage areas (ORDOÑEZ-LUCENA et al., 2017).

In this hybrid phase, operators deploy combined data functions, such as Dual-stack PGW-C/SMF instances for the control plane and PGW-U/UPF for the service plane. user. These functions are able to simultaneously process the 4G GTPv2 protocols and the HTTP/2 and PFCP procedures of 5G SA, simplifying the consolidation of databases of subscribers at UDR.

The third phase is the Native 5G SA (Option 2 Full) stage, in which the legacy 4G core... It is progressively deactivated, and all mobile traffic is absorbed by the architecture. SBA based on CNFs. Achieving this phase requires the massive migration of SIM cards and User devices for profiles compatible with 5G SA technology.

The technical validation of each migration step requires a rigorous testing program. In addition to functional tests to ensure compliance with 3GPP standards, the teams of Engineering teams must perform extreme load tests and resilience simulations using... Fault injection testing (Chaos Engineering). This approach allows for the identification of... Previously, it was explored how the microservices mesh reacts to sudden losses of computing nodes or sudden degradations in connectivity (ORDOÑEZ-LUCENA et al., 2017).

Final Considerations

Transforming the core of mobile networks into a cloud-native architecture.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.1 2026 | Submission: 02/14/2026 | Accepted: 02/17/2026 | Publication: 02/20/2026

Service-based engineering represents the most profound innovation that has occurred in engineering. Telecommunications in the last decade. The decomposition of the control plane into microservices. Decoupled instances and the migration of physical instances to virtual containers establish the an indispensable foundation to support advanced applications and the extreme diversity of Projected demands for the 5G ecosystem.

As demonstrated throughout this analysis, the gains in flexibility, The scalability and speed of deployment brought by CNFs do not constitute benefits. Automatic or isolated. The elimination of the traditional legacy black box model introduces a substantial layer of software complexity, transferring the engineering challenge to Physical hardware for coordinating distributed ecosystems.

The stability and resilience of 5G Core are intrinsically dependent on the maturity of... Communication network oriented towards Service-Based Architecture (SBA). Decoupling Effective integration between control and data via CUPS and decoupled state storage in UDR These are the cornerstones that allow the system to withstand partial infrastructure failures without to impact subscriber connectivity.

In the context of cybersecurity, opening internal interfaces to APIs HTTP/2 requires a paradigm shift towards a Zero Trust architecture. The implementation of mTLS, authorization via OAuth 2.0, and the use of Service Mesh with sidecar proxies are no longer necessary. They were optional and are now considered mandatory requirements to contain threats and prevent Lateral movements in the microservices network.

In parallel, lifecycle automation under Kubernetes orchestration and the The ETSI NFV MANO model is the only viable way to manage the scale of these. deployments. The ability to perform HPA autoscaling, self-healing and Progressive updates without service interruption are what enable operational efficiency. and the economic sustainability of contemporary operators.

Contextualized observability emerges as the indispensable discipline for governing. This complexity. The sovereign integration of the three pillars — metrics, distributed tracking with W3C Trace Context and real-time event logs — provides visibility necessary to transform operational data into preventive diagnoses, isolating Failures quickly occur in environments composed of multiple vendors.

The gradual migration process from 4G EPC through NSA models and functions. Hybrid interworking models demonstrate that technological evolution requires continuous planning. A secure transition to native 5G SA requires rigorous API contract governance.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Machine Translated by Google

RCMOS – Multidisciplinary Scientific Journal The Knowledge.
ISSN: 2675-9128. São Paulo-SP.

Year VII, v.1 2026 | Submission: 02/14/2026 | Accepted: 02/17/2026 | Publication: 02/20/2026

Continuous compliance testing and proactive infrastructure validation through Fault injection methodologies.

In conclusion, the degree of technical maturity of a cloud-native 5G Core should not to be measured solely by the number of virtualized functions or by the theoretical rate of Network transmission. It is revealed in the ability of engineering teams to control the Software complexity, ensuring seamless interoperability, and guaranteeing reliability. total service even in adverse scenarios of failure and high demand.

References

3GPP. TS 23.501: System architecture for the 5G System; Stage 2 (Release 18). Sophia Antipolis: 3GPP, 2024a. Available at: https://www.3gpp.org/dynareport/23501.htm.

3GPP. TS 23.502: Procedures for the 5G System; Stage 2 (Release 18). Sophia Antipolis: 3GPP, 2024b. Available at: https://www.3gpp.org/dynareport/23502.htm.

3GPP. TS 29.500: Technical realization of Service Based Architecture; Stage 3 (Release 18). Sophia Antipolis: 3GPP, 2024c. Available at: https://www.3gpp.org/dynareport/29500.htm.

3GPP. TS 33.501: Security architecture and procedures for 5G System (Release 18). Sophia Antipolis: 3GPP, 2024d. Available at: https://www.3gpp.org/dynareport/23501.htm.

BARAKABITZE, AA et al. 5G network slicing using SDN and NFV: a survey of taxonomy, architectures and future challenges. Computer Networks, vol. 167, p. 106984, 2020. DOI: https://doi.org/10.1016/j.comnet.2019.106984.

BONDAN, L. et al. Survey of network virtualization orchestration solutions. Computer Communications, vol. 94, p. 79-91, 2016. DOI: https://doi.org/10.1016/j.comcom.2016.09.015.

ETSI. GS NFV 002 V1.2.1: Network Functions Virtualization Architectural Framework. Sophia Antipolis: ETSI, 2014. Available at: https://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.02.01_60/gs_NFV002v010201p.pdf.

ITU. Measuring digital development: Facts and Figures 2024. Geneva: International Telecommunication Union, 2024. Available at: https://www.itu.int/itu-d/reports/statistics/facts-figures-2024/.

KREUTZ, D. et al. Software-defined networking: a comprehensive survey. Proceedings of the IEEE, vol. 103, no. 1, p. 14-76, 2015. DOI: https://doi.org/10.1109/JPROC.2014.2371999.

NIST. SP 800-204A: Building secure microservices-based applications using service-mesh architecture. Gaithersburg: NIST, 2020. DOI: https://doi.org/10.6028/NIST.SP.800-204A.

ORDOÑEZ-LUCENA, J. et al. Network slicing for 5G with SDN/NFV: concepts, architectures, and challenges. IEEE Communications Magazine, vol. 55, n. 5, p. 80-87, 2017. DOI: https://doi.org/10.1109/MCOM.2017.1600935.

YILMA, GM et al. On the challenges and KPIs for benchmarking open-source NFV MANO systems. In: PROCEEDINGS OF IEEE NETSOFT, 2019, Paris. Annals [...]. IEEE, 2019. p. 1-9. DOI: https://doi.org/10.1109/NETSOFT.2019.8806670.

This article is published in open access under the Creative Commons Attribution license, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.