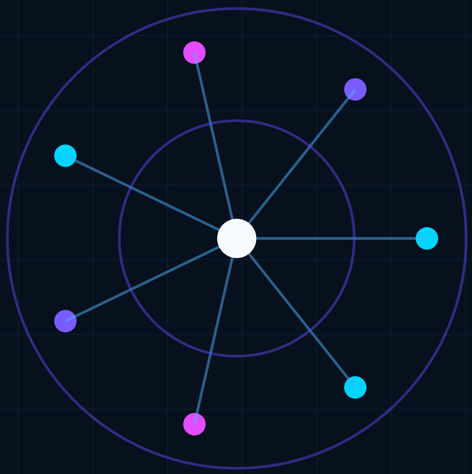
MYTHOS SYSTEMS

TECHNICAL LIBRARY / RESEARCH INTELLIGENCE

5G AND 6G NETWORKS

5G/6G Network Slicing & QoS Enforcement

Current-source review, evidence-bounded adoption decision, explicit limitations, reproducibility controls, and preserved source research note.



PERMANENT ID	EVIDENCE	ADOPTION	FRESHNESS
RES-028	A-	ADOPT 5G CONTROLS; MONITOR 6	ACTIVE WATCH

Freshness review: 2026-09-17 / Next scheduled review: 2026-12-16

CANDIDATE RESEARCH REPORT / 2.1.0-CANDIDATE / PUBLIC

RESEARCH CONTROL SURFACE

Required Research Fields

Each field remains independently reviewable; evidence strength does not imply production authority.

EVIDENCE GRADE — **A-**

Strength of the retained source set and technical basis.

SOURCE AUTHORITY — **2 registered authorities**

3GPP TS 23.501 - System Architecture for the 5G System; 3GPP Release 21 Timeline

FRESHNESS — **ACTIVE WATCH**

Reviewed 2026-09-17; dynamic sources require event-driven revalidation.

CONFLICTS — **VISIBLE / NOT SILENT**

Differences between specification, vendor behavior, research claims, and reproduced evidence must remain explicit.

LIMITATIONS — **EXPLICIT**

No certification, procurement approval, legal conclusion, or unbounded production claim is created by this report.

REPRODUCIBILITY — **REQUIRED**

Material claims require exact versions, representative data, failure cases, artifacts, and repeatable acceptance criteria.

ADOPTION POSTURE — **ADOPT 5G CONTROLS; MONITOR 6G**

Adopt explicit end-to-end 5G slice assurance and QoS verification where slicing is used. Treat 6G architecture and Release 21 material as evolving research and standards work.

REVIEW TRIGGER — **2026-12-16**

Scheduled at 90 days; earlier on material source, vulnerability, implementation, or contradictory-evidence change.

SOURCE AUTHORITY / FRESHNESS

Authority Register and Freshness Delta

Primary-source lineage is preserved; current-source changes are separated from unperformed implementation claims.

AUTHORITY 01

3GPP TS 23.501 - System Architecture for the 5G System

https://www.3gpp.org/dynareport/23501.htm

AUTHORITY 02

3GPP Release 21 Timeline

https://www.3gpp.org/news-events/3gpp-news/rel21-timeline

2026-09-17 FRESHNESS DELTA

3GPP Release 19 is frozen; Releases 20 and 21 remain open. 6G assertions therefore require release-specific qualification.

Freshness policy: scheduled review + immediate review on source supersession, material release, vulnerability, retraction, or contradictory evidence.

Evidence Must Survive Contact With Reality

SOURCE
authority

CLAIM
bounded

TEST
representative

EVIDENCE
retained

DECISION
conditional

- Source authority is not implementation evidence. Product behavior, scale, security, interoperability, and operator fit remain environment-specific.

- Conflicting evidence is recorded rather than averaged away. Specification behavior, vendor implementation, preprint results, and production observations are separate evidence classes.

- Quantitative claims are informative until reproduced under documented hardware, software, data, topology, load, and failure conditions.

- Adoption posture is reversible. A stronger source set can coexist with a pilot-only or research-only recommendation when maturity, safety, economics, or operability remain unresolved.

Decision Gate and Validation Plan

ADOPTION POSTURE

ADOPT 5G CONTROLS; MONITOR 6G

Adopt explicit end-to-end 5G slice assurance and QoS verification where slicing is used. Treat 6G architecture and Release 21 material as evolving research and standards work.

1 / SOURCE	Pin exact versions, publication state, retrieved artifacts, and source hashes.
2 / PROTOTYPE	Demonstrate the core mechanism with representative data and instrumented execution.
3 / FAILURE	Exercise malformed input, dependency loss, stale state, overload, recovery, rollback, and misuse.
4 / BASELINE	Compare against an incumbent, classical, or simpler architecture using the same workload.
5 / ACCEPT	Record acceptance criteria, residual limitations, owner, expiration, and revalidation triggers.

EXPIRATION / REVIEW TRIGGER

Next scheduled review: 2026-12-16 (90-day cadence). Review sooner after material source revision, breaking implementation release, critical vulnerability, retraction, benchmark contradiction, changed workload, or changed legal/safety boundary.

8. Complete Source Research Note

SOURCE-LINEAGE NOTICE

The following material preserves the complete original source note, excluding only the conversational wrapper and outer Markdown fence. Legacy status labels and absolute language are retained for traceability and do not override the candidate status, limitations, or adoption decision in this edition.

Document ID: RES-028 Version: 1.0.0 (Definitive Registry Edition) Status: Published Research Note Classification: Public Organization: Mythos Systems (MYTHOS AI) Owner: Aaron Stovall Effective Date: 2026-07-16 Applies To: Telecom architects, private 5G network engineers, industrial IoT specialists, and AI engineers designing ultra-reliable low-latency communication (URLLC) pipelines for physical AI and sovereign edge compute Companion Standards: MYTHOS-TEL-0001 (5G/6G Core, Open RAN & Slicing), MYTHOS-ROB-0001 (Physical AI & Autonomous Fleets), MYTHOS-IOT-0001 (IoT & Edge Sensors), MYTHOS-SEC-0007 (Microsegmentation), MYTHOS-NET-0004 (Zero-Trust Networking)

The architecture of wireless broadband has failed. Organizations attempt to support divergent workloads—autonomous robotics requiring sub-10ms latency, and massive video streams requiring gigabit bandwidth—over a single, "best-effort" RF network. They attempt to manage traffic using DiffServ/QoS tags, which is a prioritization suggestion, not a physical guarantee. When a massive video download saturates the cell tower, the autonomous robot's control link drops, resulting in a physical crash.

5G Standalone (SA) Network Slicing shatters this best-effort paradigm. A network slice is not a VLAN or a QoS tag; it is a logically isolated, end-to-end network built over a shared physical infrastructure. It spans from the device (UE), through the Radio Access Network (RAN), across the transport fabric, and through dedicated 5G Core (5GC) functions.

This research note defines the architectural dynamics of 5G/6G Network Slicing. It dissects the mechanics of NSSAI (Network Slice Selection Assistance Information), the hard reservation of Physical Resource Blocks (PRBs) at the RAN MAC scheduler, and the strict isolation of User Plane Functions (UPF) to guarantee mathematically bounded SLAs. Understanding these dynamics is a prerequisite for building the sovereign, physical AI, and industrial IoT fabrics mandated by the Mythos Telecom Standards.

To understand slicing, we must move from prioritization tags to dedicated, virtualized network functions bound to specific radio resources.

1.1 The S-NSSAI (The Slice ID)

A 5G device does not just connect to a network; it requests a specific slice.

- The Mechanic: The device sends a registration request containing its requested NSSAI (Network Slice Selection Assistance Information). The 5G Core’s Access and Mobility Management Function (AMF) evaluates this request and routes the device to the specific Slice/Session Management Function (SMF) and User Plane Function (UPF) dedicated to that slice.

1.2 End-to-End Isolation (RAN + Transport + Core)

A true network slice is not just a core construct; it spans the entire physical network.

- RAN Slicing: The gNodeB (base station) reserves specific Physical Resource Blocks (PRBs)—the actual time/frequency units of the RF spectrum—exclusively for the slice.
- Transport Slicing: The fronthaul and backhaul network (typically SRv6 or MPLS) provisions dedicated, traffic-engineered paths with guaranteed bandwidth and latency for the slice.
- Core Slicing: The 5GC spins up dedicated UPF (User Plane Function) instances, either in the cloud or at the edge, specifically to process the traffic for that slice, completely isolating the data plane from other slices.

1.3 The 3GPP Slice Types (eMBB, URLLC, mMTC)

5G defines standardized slice types to match the physics of the RF to the application:

- eMBB (Enhanced Mobile Broadband): Optimized for high throughput (e.g., 4K video, massive data dumps). Prioritizes bandwidth over latency.
- URLLC (Ultra-Reliable Low-Latency Communication): Optimized for sub-10ms latency and 99.999% reliability (e.g., physical robotics, autonomous vehicles, remote surgery). Prioritizes latency over bandwidth.
- mMTC (Massive Machine Type Communications): Optimized for millions of low-power, low-data sensors (e.g., smart meters).

While network slicing promises isolation, the underlying RF spectrum is a shared, physical medium. This introduces severe physical and mathematical constraints.

2.1 The "Soft" Slicing Fallacy (Noisy Neighbor)

Many early 5G deployments implement "soft slicing." They share the RAN PRBs among all slices and use QoS prioritization to give URLLC traffic preference.

- The Flaw: If an eMBB slice is saturating the RAN with a massive download, the URLLC traffic gets priority, but it still must wait in the MAC scheduler queue behind the eMBB packets already being transmitted. The latency spike violates the URLLC SLA.
- The Mitigation: True slicing MUST utilize "hard" RAN slicing. The MAC scheduler MUST physically partition the PRBs. For example, 80% of PRBs go to eMBB, 20% are strictly reserved for URLLC. The eMBB slice cannot use the URLLC PRBs, even if they are idle. This guarantees URLLC latency bounds.

2.2 The Inter-Slice Pivot Threat

If a slice is compromised (e.g., a massive IoT sensor botnet is breached), the attacker might attempt to pivot from the mMTC slice into the URLLC slice controlling the factory robotics.

- The Flaw: If all slices share a common UPF or a common GTP-U (GPRS Tunneling Protocol) gateway, a compromise of the shared infrastructure breaks the isolation.
- The Mitigation: Each slice MUST possess dedicated, microsegmentated UPF instances. Inter-slice communication MUST be blocked by default and routed through a highly scrutinized, policy-enforced Application Function (AF) gateway.

2.3 The Spectrum Exhaustion Ceiling

RF spectrum is finite. A cell tower has a hard physical limit (e.g., 100 MHz of bandwidth).

- The Constraint: If you allocate 20 MHz to URLLC, that spectrum is permanently unavailable to eMBB. Over-provisioning hard slices starves the network of general-purpose capacity.

The true power of 5G/6G slicing is realized when hard RAN partitioning is combined with edge compute, creating mathematically deterministic data planes.

3.1 URLLC and Time-Sensitive Networking (TSN)

For industrial robotics (`MYTHOS-ROB-0001`), a 5G slice can be configured as a TSN bridge.

- The Mechanic: The URLLC slice utilizes specific 5G numerologies (e.g., mini-slots) that reduce transmission time intervals (TTI) to less than 1ms. Combined with edge compute (MEC) deployed at the base station, the round-trip latency from sensor to AI agent to actuator is physically bounded to under 10ms.

- The Impact: The factory floor replaces miles of rigid physical Ethernet cabling with wireless 5G URLLC, allowing robots to move freely without losing deterministic control.

3.2 Network Slicing as Zero-Trust Microsegmentation

In a Mythos-compliant architecture, a 5G slice is treated as the ultimate physical zero-trust boundary.

- The Mechanic: A smart camera (eMBB slice) and an industrial valve (URLLC slice) might be in the same physical room, connected to the same gNodeB. However, because their NSSAI differs, they are routed to completely different UPFs, different subnets, and different firewalls. The camera is physically incapable of addressing the valve.

The fundamental shift of network slicing is the viability of Private 5G as a sovereign enterprise fabric.

- The Industrial Metaverse: A manufacturing plant deploys a Private 5G network. They provision a URLLC slice for AGVs (Automated Guided Vehicles), an eMBB slice for AR (Augmented Reality) headsets worn by maintenance workers, and an mMTC slice for environmental sensors. All coexist on one RF spectrum without interfering.
- First Responder Priority: In a public 5G network, a slice is reserved for emergency services. During a disaster when civilian eMBB traffic saturates the tower, the first responder URLLC slice operates flawlessly on its reserved PRBs.
- Bounded SLA AI Inference: An autonomous AI agent requires cloud inference but cannot tolerate internet latency. A dedicated 5G slice connects the agent directly to a localized MEC (Multi-access Edge Computing) datacenter, guaranteeing a 5ms end-to-end RTT.

To deploy 5G slicing in production, the Mythos Architecture enforces strict isolation, GTP-U inspection, and edge compute boundaries.

5.1 Dedicated UPF Microsegmentation

The 5G Core MUST NOT use a monolithic UPF for all slices.

- The Mitigation: The Mythos standard mandates dedicated, containerized UPFs (cUPF) deployed at the edge for each critical slice. The cUPF is treated as a zero-trust workload, integrated with a Service Mesh (Istio/Linkerd) to enforce mTLS and L7 authorization on all downstream API calls.

5.2 GTP-U Firewalling

The GTP-U (GPRS Tunneling Protocol - User Plane) tunnels traffic between the RAN and the Core.

- The Mitigation: The architecture MUST implement a 5G-aware firewall (e.g., Palo Alto Networks or Cisco 5G Secure Gateway) that inspects the GTP-U headers. It must drop any GTP-U packet where the NSSAI (slice ID) does not match the expected source/destination tunnel endpoints, preventing cross-slice pivoting.

5.3 Hard PRB Reservation Verification

The RAN MAC scheduler configuration MUST be verified.

- The Mitigation: The continuous reconciliation plane (NetBox/Ansible) MUST audit the gNodeB configuration. If an engineer accidentally configures soft slicing (shared PRBs) for a URLLC slice, the pipeline must detect the deviation and auto-revert the configuration to hard slicing before a robotic failure occurs.

The strategy of treating wireless networks as best-effort pipes is obsolete for the era of physical AI and industrial automation. 5G/6G Network Slicing, powered by Standalone cores and hard RAN partitioning, transforms the shared RF spectrum into a deterministic, mathematically bounded fabric. By dedicating radio resources, transport paths, and core functions to specific workloads, we guarantee that a massive video stream will never cause a physical robot to crash. In a Mythos-compliant architecture, the slice is not a QoS tag; it is an absolute physical boundary.

```
A QoS tag is a suggestion; a hard PRB reservation is a physical law.
A shared UPF is a pivot vector; a dedicated UPF is a boundary.
```

```
A best-effort network drops packets; a sliced network guarantees delivery.

The spectrum is shared; the slice is absolute.

> RF may be physical.
> Slice isolation must be absolute.
```

End of Research Note RES-028

9. Source Register

Source	Authority and Status	Freshness Control
3GPP TS 23.501 - System Architecture for the 5G System https://www.3gpp.org/dynareport/23501.htm	Primary telecom specification Versioned and actively maintained Published: Living	Validated: 2026-07-22 Review on material revision, withdrawal, supersession, or scheduled report review.
3GPP Release 21 Timeline https://www.3gpp.org/news-events/3gpp-news/rel21-timeline	Primary standards-program update Current planning baseline Published: 2026	Validated: 2026-07-22 Review on material revision, withdrawal, supersession, or scheduled report review.

10. Lineage, Review, and Publication Record

Record	Value
Original source file	RES-028_5G_6G_Network_Slicing_QoS_Enforcement.md
Original source words	1605
Upgrade type	Enterprise research report; source and freshness validation; limitations; adoption decision; reproducibility plan
Generated on	2026-07-22
Current status	Candidate Research Report
Publication authority	Formal Mythos approval not yet recorded
Next review	90 days or event-driven trigger, whichever occurs first