MYTHOS SYSTEMS

PERMANENT LIBRARY PUBLICATION

ENGINEERING STANDARDS LIBRARY / NETWORK ENGINEERING

5G, 6G, RAN Automation, and Network Slicing Standard

Defines mobile architecture, orchestration, slicing, isolation, QoS, telemetry, and research boundaries.

PERMANENT DOCUMENT ID
MYTHOS-NET-0007

PUBLICATION
Candidate Standard

ASSURANCE SURFACE
9 Atomic Criteria / 6 Families

PERMANENT PUBLICATION IDENTITY

5G, 6G, RAN Automation, and Network Slicing Standard

Defines mobile architecture, orchestration, slicing, isolation, QoS, telemetry, and research boundaries.

DOCUMENT ID
MYTHOS-NET-0007

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-23

SCHEDULED REVIEW
2027-01-23

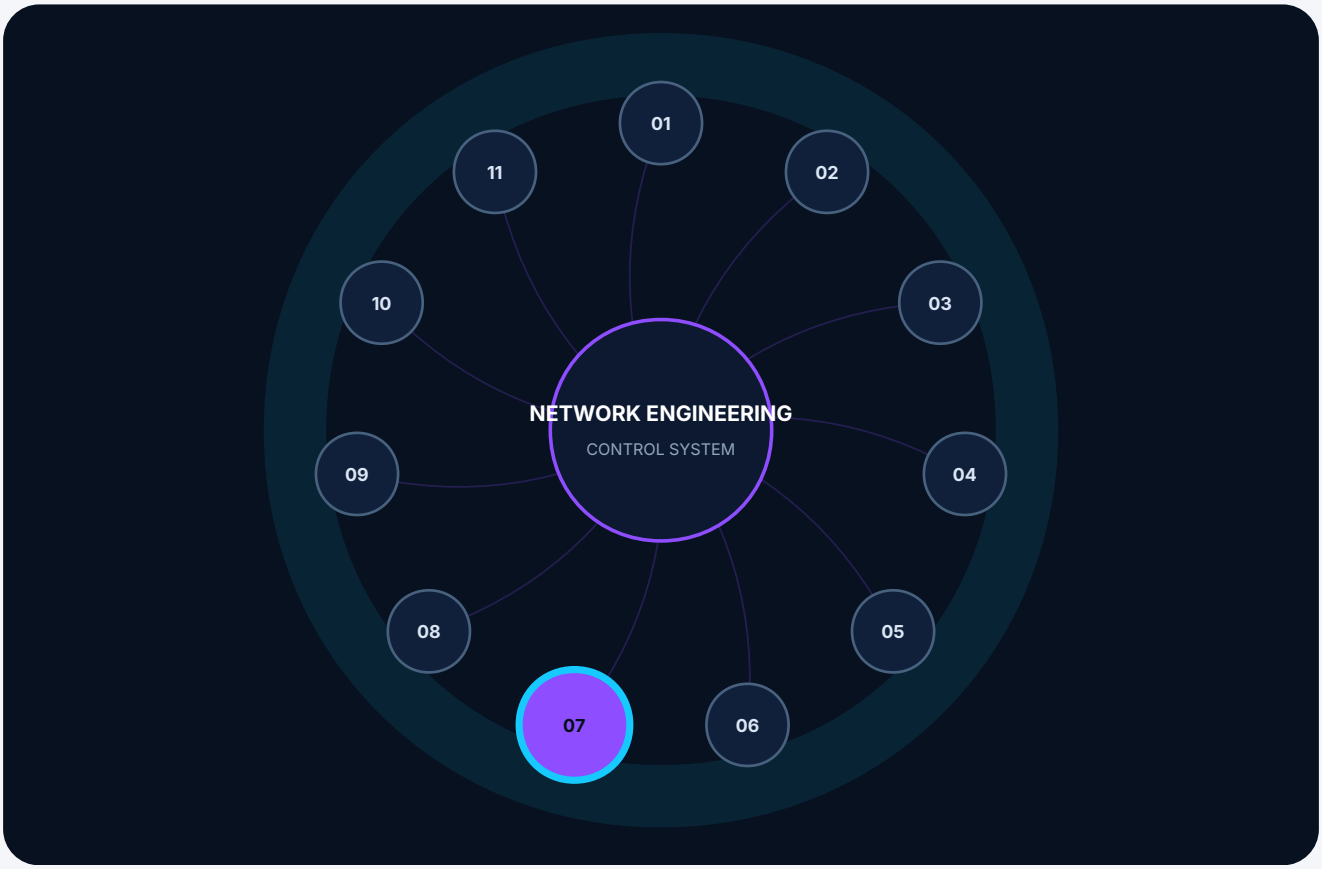
CLASSIFICATION
Public

9	6	4	1
ATOMIC CRITERIA	CAPABILITY FAMILIES	ASSESSMENT PROFILES	PERMANENT IDENTITY

Publication doctrine. This standard establishes durable requirements for its defined scope. Interpretation must preserve the permanent document identity, recorded evidence, and formal revision history.

DOMAIN CONTROL SYSTEM

MYTHOS-NET-0007 inside the network engineering standard constellation



Connected assurance

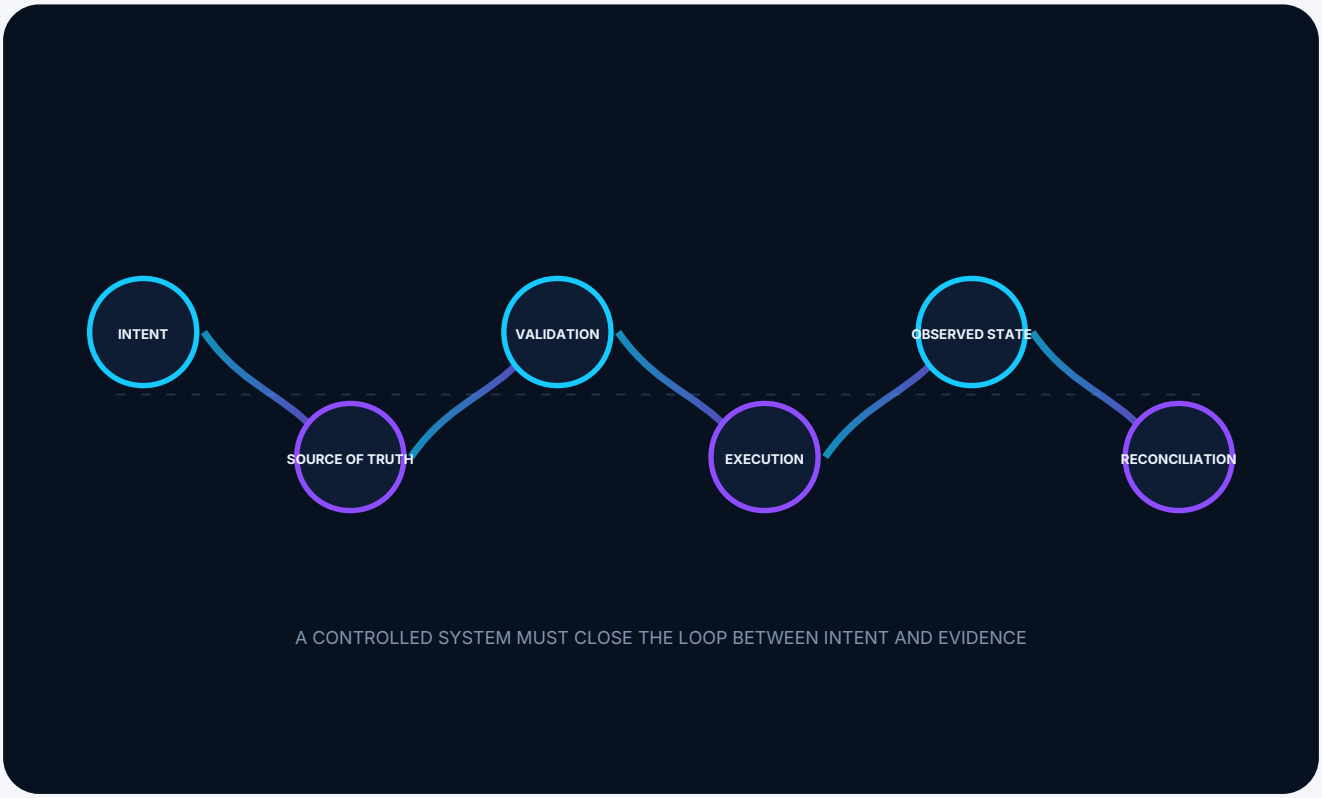
Architecture, policy, implementation, operations, and evidence are evaluated as one controlled system.

Specialization rule

Companion standards may add precision, but they cannot silently weaken this publication's requirements.

CLOSED-LOOP ARCHITECTURE

Intent becomes trustworthy only when observed state returns as evidence



State separation

Desired, approved, deployed, observed, historical, and simulated states must remain distinguishable.

Recoverable change

Material change requires validation, authorization, monitoring, containment, and a credible recovery path.

EVALUATION TOPOLOGY

The capability families and atomic criteria of MYTHOS-NET-0007

Capability families

Families expose the major engineering surfaces and preserve the source weighting model.

Atomic criteria

Each criterion carries a question, maturity spectrum, evidence expectations, assessment method, and operational signals.

NAVIGATION

Contents

ENGINEERING DOCTRINE

0. Executive Mandate

The deployment of 5G and emerging 6G networks has failed to deliver on the promise of programmable wireless infrastructure.

Telecom operators have built 5G networks as fatter 4G pipes, utilizing standalone macro cells and monolithic, vendor-locked RAN stacks. Network slicing remains a theoretical construct confined to core network (5GC) QoS markers, completely ignoring the radio resource bottleneck. Best-effort wireless is fundamentally incompatible with the deterministic latency requirements of autonomous industrial systems (IIoT), real-time robotics, and sovereign edge AI.

This standard exists because:

1. **Best-Effort Wireless is a Liability:** Marking QCI/5QI values in the 5G Core does not guarantee radio resources. If the RAN is congested, URLLC packets drop. Slicing MUST extend all the way to the scheduler on the radio cell.
2. **Monolithic RAN is Vendor Lock-in:** Proprietary baseband units (BBUs) and remote radio heads (RRHs) from a single vendor stifle innovation and prevent the deployment of AI-driven radio optimization. O-RAN (Open RAN) decouples hardware from software, enabling RAN Intelligent Controllers (RICs) to optimize the radio in real-time.
3. **Edge AI Requires Deterministic Uplink:** AI inference at the edge (MEC) is useless if the sensor data cannot reach the edge node within strict latency bounds. 6G and 5G-Advanced must provide sub-millisecond jitter and 99.999% reliability for URLLC.
4. **Spectrum is a Finite Sovereign Asset:** Dynamic Spectrum Sharing (DSS) and CBRS-style shared spectra require AI-driven allocation to prevent interference and maximize utilization.

This document establishes the **Mythos RAN & Slicing Standard (MRSS)**, a comprehensive, evidence-based methodology for evaluating 5G/6G networks against slicing isolation, O-RAN programmability, and deterministic latency criteria.

ENGINEERING DOCTRINE

Part I. Scope and Applicability

1.1 In Scope

This standard covers the evaluation of:

- 5G/6G Network Slicing (Core, Transport, and RAN slicing)
- Open RAN (O-RAN) architecture (O-CU, O-DU, O-RU, SMO)
- RAN Intelligent Controllers (Non-RT RIC, Near-RT RIC, xApps, rApps)
- Ultra-Reliable Low-Latency Communication (URLLC) determinism
- Multi-access Edge Computing (MEC) and UPF breakout integration
- Spectrum management and Dynamic Spectrum Sharing (DSS)

1.2 Out of Scope

- General transport architecture (covered in MYTHOS-NET-0006)
- General edge compute sandboxing (covered in MYTHOS-EMT-0001)
- Broad telecom billing and roaming (reserved for future MYTHOS-TEL domain)

1.3 Audience

- Network architects designing private 5G/6G and O-RAN fabrics
- IIoT and operational technology (OT) engineers requiring deterministic wireless
- AI/ML engineers building RIC xApps/rApps
- Defense and sovereign infrastructure operators
- Standards bodies seeking a reference RAN/slicing methodology

---

ENGINEERING DOCTRINE

Part II. Definitions and Taxonomy

2.1 RAN and Slicing Dimensions

Dimension	Definition
Network Slice	An end-to-end logical network spanning Core (5GC), Transport, and RAN, providing specific QoS (e.g., URLLC, eMBB, mMTC) with isolated resources.
O-RAN	Open Radio Access Network. An architecture that disaggregates the RAN into O-CU (Centralized Unit), O-DU (Distributed Unit), and O-RU (Radio Unit) with open fronthaul interfaces.
RIC	RAN Intelligent Controller. An AI/ML-driven orchestration layer (Near-RT for sub-ms scheduling, Non-RT for policy) that optimizes RAN performance via xApps and rApps.
URLLC	Ultra-Reliable Low-Latency Communication. A 5G service category targeting sub-1ms latency and 99.999% reliability.
MEC	Multi-access Edge Computing. Hosting compute/AI resources at the cellular base station or aggregation site for local data breakout.

2.2 The Wireless Doctrine

> A pipe is not a platform. Best-effort is not a slice. Proprietary RAN is vendor lock-in. A slice that does not reserve radio resources is a VLAN. Wireless must be deterministic.

ENGINEERING DOCTRINE

Part III. Evaluation Methodology

3.1 Scoring Model

Each capability is scored from 0 to 5.

Score	Meaning
0	Fails basic task; monolithic RAN, best-effort only, no slicing
1	Basic 5GC QoS, but no RAN slicing or O-RAN
2	Functional slicing but lacks RAN isolation or RIC automation
3	Solid production performance; O-RAN, RIC, RAN slicing
4	Strong performance; deterministic URLLC, AI-driven RIC
5	Best-in-class; sets the standard for autonomous, 6G-ready wireless

Weighting

Category	Weight	Rationale
Network Slicing & Radio Isolation	25%	A slice without radio resources is a lie
O-RAN & RIC Automation	20%	Monolithic RAN cannot scale or optimize dynamically
URLLC & Deterministic Latency	20%	IIoT/Autonomy requires mathematical latency bounds
Edge Integration (MEC/UPF)	15%	Edge AI requires local breakout
Spectrum & Interference Management	10%	Shared spectrum requires AI governance
Operational Lifecycle & Security	10%	RIC/xApps are a new attack surface

Total: 100%

A system MUST score at least 3.0 in Network Slicing and URLLC to be considered for production use in regulated/industrial environments.

EVALUATION AND ASSURANCE SYSTEM

Capability claims are bounded by evidence, context, and reproducible assessment.

9 atomic criteria across 6 capability families define the evaluation surface of this standard.

4.1 / CAPABILITY FAMILY

Network Slicing and Radio Isolation

SOURCE WEIGHT 25%

4.1.1
End-to-End Slice Isolation

4.1.2
Slice Lifecycle Management

MYTHOS-NET-0007-EVAL-4.1.1

End-to-End Slice Isolation

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Network Slicing and Radio Isolation	**4.1.1**	**25%**	**Evidence-led**

Does the slice guarantee isolated resources from the Core through the Transport to the RAN scheduler?

0
No slicing; best-effort QoS marking only

1
5GC slicing (UPF/AMF isolation) but shared RAN scheduler

2
Soft RAN slicing (QoS prioritization, but no hard resource reservation)

3
Hard RAN slicing (dedicated PRBs/ Resource Blocks per slice)

4
Hard RAN slicing + Transport slicing (SRv6/I-SID) + Core isolation

5
Leading isolation: mathematically proven end-to-end resource isolation, zero cross-slice interference under congestion, formally verified SLAs

ENGINEERING INTERPRETATION

This criterion evaluates whether end-to-end slice isolation is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- source-of-truth objects, Git history, observed-state snapshots, and reconciliation evidence
- approved architecture or policy record
- current configuration or platform export

ASSESSMENT PROCEDURE

1. introduce controlled drift and verify detection, adjudication, and restoration
2. Examine authoritative design, policy, configuration, and lifecycle records.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- multiple authorities, silent manual changes, stale inventory, and destructive auto-remediation
- The control exists only in diagrams or policy text.

OPERATIONAL MEASURES

- drift detection time
- reconciliation success
- unowned object count
- coverage of in-scope assets or flows

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

MYTHOS-NET-0007-EVAL-4.1.2

Slice Lifecycle Management

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Network Slicing and Radio Isolation	4.1.2	25%	Evidence-led

Can slices be instantiated, modified, and terminated programmatically?

0
Manual provisioning

1
Template-based core slicing via OSS

2
API-driven core and transport slicing

3
Automated E2E slice provisioning including RAN parameters

4
Dynamic slice scaling based on real-time demand (RIC-driven)

5
Leading lifecycle: intent-driven slice creation, formally verified SLA compliance, AI-driven dynamic re-slicing in sub-second intervals

ENGINEERING INTERPRETATION

This criterion evaluates whether slice lifecycle management is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.2 / CAPABILITY FAMILY

O-RAN and RIC Automation

SOURCE WEIGHT 20%

4.2.1
RIC Architecture

4.2.2
xApp/rApp Ecosystem

MYTHOS-NET-0007-EVAL-4.2.1

RIC Architecture

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
O-RAN and RIC Automation	4.2.1	20%	Evidence-led

Does the network implement an O-RAN compliant RAN Intelligent Controller?

0
Monolithic vendor RAN; no RIC

1
Vendor-specific AI optimization (black box)

2
Non-RT RIC implemented for policy and rApps

3
Near-RT RIC implemented for sub-ms scheduling and xApps

4
Full O-RAN stack (SMO, Non-RT, Near-RT) with open xApp/rApp ecosystem

5
Leading RIC: formally verified xApp/rApp sandboxing (WASM), AI-driven intent translation, and zero vendor lock-in

ENGINEERING INTERPRETATION

This criterion evaluates whether ric architecture is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

MYTHOS-NET-0007-EVAL-4.2.2

xApp/rApp Ecosystem

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
O-RAN and RIC Automation	4.2.2	20%	Evidence-led

Can third-party or custom AI applications (xApps/rApps) be safely deployed to the RIC?

0
No third-party extensibility

1
Vendor-approved apps only

2
Side-loaded apps with no isolation

3
Containerized apps with resource limits

4
WASM-sandboxed xApps with AIBOM and behavioral verification

5
Leading ecosystem: formally verified sandboxing, zero resource starvation, cryptographic attestation of app provenance, and automated rollback

ENGINEERING INTERPRETATION

This criterion evaluates whether xapp/rapp ecosystem is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.3 / CAPABILITY FAMILY

URLLC and Deterministic Latency

SOURCE WEIGHT 20%

4.3.1
Latency Guarantees

4.3.2
Time Sensitive Networking (TSN) Integration

MYTHOS-NET-0007-EVAL-4.3.1

Latency Guarantees

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
URLLC and Deterministic Latency	4.3.1	20%	Evidence-led

Can the network mathematically guarantee sub-ms latency for URLLC slices?

0
No latency guarantees; statistical best-effort

1
Target latency defined, but unverified under load

2
Latency verified in lab conditions

3
Latency verified under simulated congestion (digital twin)

4
Deterministic scheduling (e.g., 5G TSN integration, mini-slots)

5
Leading URLLC: formally verified sub-ms determinism, 99.999% reliability, zero jitter under adversarial load, and hardware-accelerated scheduling

ENGINEERING INTERPRETATION

This criterion evaluates whether latency guarantees is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

MYTHOS-NET-0007-EVAL-4.3.2

Time Sensitive Networking (TSN) Integration

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
URLLC and Deterministic Latency	4.3.2	20%	Evidence-led

Does the 5G network integrate with industrial TSN networks for deterministic wired/wireless convergence?

0
No TSN awareness

1
Basic TSN translation at the edge

2
5G TSN Translator (DS-TT/NW-TT) compliant

3
Integrated TSN scheduling (802.1Qbv) with 5G slot coordination

4
Sub-microsecond time synchronization (IEEE 1588/802.1AS) across wireless and wired

5
Leading convergence: formally verified end-to-end determinism, zero timing drift, and AI-driven schedule optimization

ENGINEERING INTERPRETATION

This criterion evaluates whether time sensitive networking (tsn) integration is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- RF survey, channel and power plan, authentication logs, and client telemetry
- approved architecture or policy record
- current configuration or platform export

ASSESSMENT PROCEDURE

1. test roaming, capacity, interference, authentication, and degraded-band behavior
2. Examine authoritative design, policy, configuration, and lifecycle records.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- coverage holes, sticky clients, co-channel interference, and insecure fallback
- The control exists only in diagrams or policy text.

OPERATIONAL MEASURES

- coverage compliance
- authentication success
- roaming interruption
- airtime utilization
- coverage of in-scope assets or flows

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.4 / CAPABILITY FAMILY

Edge Integration (MEC/ UPF)

SOURCE WEIGHT 15%

4.4.1
UPF Breakout

MYTHOS-NET-0007-EVAL-4.4.1

UPF Breakout

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Edge Integration (MEC/ UPF)	4.4.1	15%	Evidence-led

Can traffic be selectively broken out at the edge (MEC) without traversing the core?

0
All traffic hairpins to central core

1
Static UPF at regional data centers

2
Dynamic UPF selection at the edge

3
UL CL (Uplink Classifier) for per-flow local breakout

4
Integrated MEC platform with local AI inference and RAN awareness

5
Leading edge: RAN-aware dynamic UPF breakout, sub-ms local routing, WASM-sandboxed edge AI, and sovereign data compliance enforcement

ENGINEERING INTERPRETATION

This criterion evaluates whether upf breakout is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.5 / CAPABILITY FAMILY

Spectrum and Interference Management

SOURCE WEIGHT 10%

4.5.1
Dynamic Spectrum Sharing

MYTHOS-NET-0007-EVAL-4.5.1

Dynamic Spectrum Sharing

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Spectrum and Interference Management	**4.5.1**	**10%**	**Evidence-led**

How efficiently is shared spectrum (e.g., CBRS) managed?

0
Static spectrum allocation only

1
Manual spectrum reconfiguration

2
SAS (Spectrum Access Server) compliant for CBRS

3
AI-driven spectrum sensing and allocation (RIC rApp)

4
Sub-ms dynamic spectrum sharing (DSS) between 4G/5G/6G

5
Leading management: AI-driven cognitive radio, formally verified interference avoidance, and zero spectrum waste

ENGINEERING INTERPRETATION

This criterion evaluates whether dynamic spectrum sharing is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

4.6 / CAPABILITY FAMILY

Operational Lifecycle and Security

SOURCE WEIGHT 10%

4.6.1
RAN Security

MYTHOS-NET-0007-EVAL-4.6.1

RAN Security

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Operational Lifecycle and Security	4.6.1	10%	Evidence-led

Is the O-RAN fronthaul and RIC protected from supply chain and runtime attacks?

0
Unauthenticated fronthaul (eCPRI) and RIC APIs

1
TLS on management interfaces

2
mTLS on fronthaul and RIC interfaces

3
Signed firmware/images for O-CU/O-DU/O-RU; xApp signing

4
Hardware roots of trust in O-RU; PQC-ready control plane

5
Leading security: formally verified fronthaul integrity, PQC-mTLS, behavioral monitoring of xApps, and zero unauthenticated radio commands

ENGINEERING INTERPRETATION

This criterion evaluates whether ran security is governed as an operating capability rather than a one-time configuration. Assessment must distinguish intended design, approved implementation, observed behavior, historical evidence, and unresolved risk.

REQUIRED EVIDENCE

- approved architecture or policy record
- current configuration or platform export
- change and exception records
- monitoring, test, or assessment evidence

ASSESSMENT PROCEDURE

1. Examine authoritative design, policy, configuration, and lifecycle records.
2. Interview the accountable owner and operators responsible for the control.
3. Test a representative positive, negative, failure, and recovery scenario.

EXAMINE - INTERVIEW - TEST

COMMON FAILURE PATTERNS

- The control exists only in diagrams or policy text.
- Observed state differs from approved intent without a governed exception.
- Evidence cannot establish scope, time, owner, or operating effectiveness.

OPERATIONAL MEASURES

- coverage of in-scope assets or flows
- age and closure rate of unresolved findings
- percentage of changes passing pre-deployment validation
- time to detect and contain control failure

DECISION BOUNDARY

A maturity score is valid only for the assessed scope and evidence period. Documentation alone does not establish operating effectiveness.

LIFECYCLE AND ASSURANCE

Part V. The Mythos RAN & Slicing Suite (MRSS)

Traditional RAN benchmarks measure throughput and coverage. The MRSS evaluates slicing isolation, deterministic latency, and RIC programmability.

5.1 Suite Composition

5.1.1 MRSS-Slicing

- **Cross-Slice Interference:** 50+ tests flooding eMBB slice to verify URLLC slice latency and packet loss remain within SLA.
- **E2E Provisioning:** 50+ tests automating slice creation via API, verifying RAN, Transport, and Core alignment.

5.1.2 MRSS-URLLC

- **Deterministic Jitter:** 100+ tests injecting RAN interference to verify sub-ms jitter bounds hold.
- **TSN Convergence:** 50+ tests verifying 1588 timing sync across wired/wireless boundaries.

5.1.3 MRSS-RIC

- **xApp Sandboxing:** 50+ tests deploying malicious/rogue xApps to verify WASM isolation and resource limits.
- **AI Optimization:** 50+ tests verifying RIC xApps improve spectral efficiency without violating slice SLAs.

5.2 Execution Protocol

PUBLICATION BOUNDARY

Candidate standard. Permanent identity. Evidence before authority.

Approval requires designated technical, security, legal, accessibility, and governance review with recorded findings and dispositions.