MYTHOS SYSTEMS

PERMANENT LIBRARY PUBLICATION

ENGINEERING STANDARDS LIBRARY / NETWORK ENGINEERING

Network Architecture, Design, and Topology Standard

Defines architecture views, topology, requirements, resilience, scale, documentation, and acceptance.

PERMANENT DOCUMENT ID
MYTHOS-NET-0001

PUBLICATION
Candidate Standard

ASSURANCE SURFACE
10 Atomic Criteria / 6 Families

PERMANENT PUBLICATION IDENTITY

Network Architecture, Design, and Topology Standard

Defines architecture views, topology, requirements, resilience, scale, documentation, and acceptance.

DOCUMENT ID
MYTHOS-NET-0001

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-23

SCHEDULED REVIEW
2027-01-23

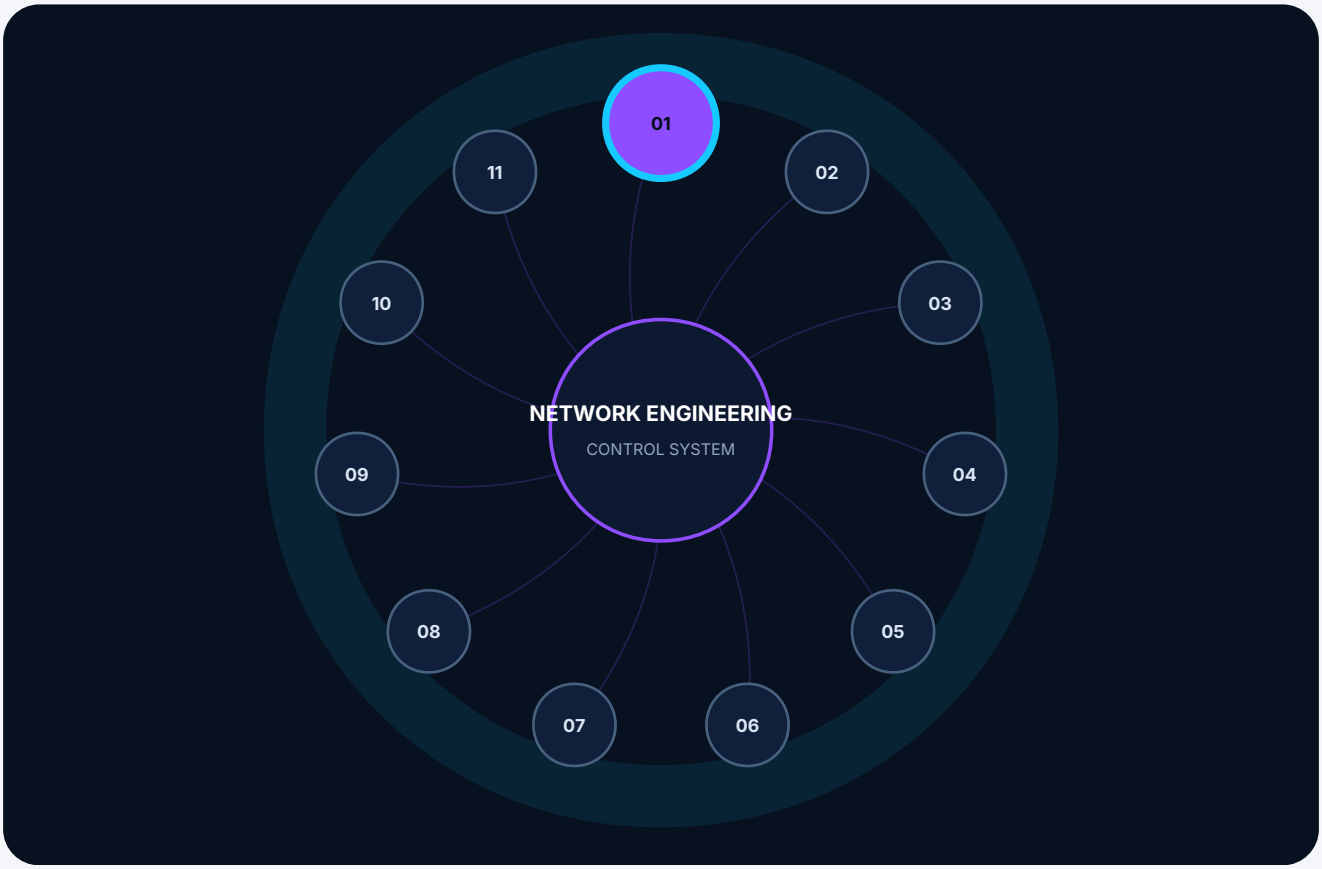
CLASSIFICATION
Public

10	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-0001 inside the network engineering standard constellation



Connected assurance

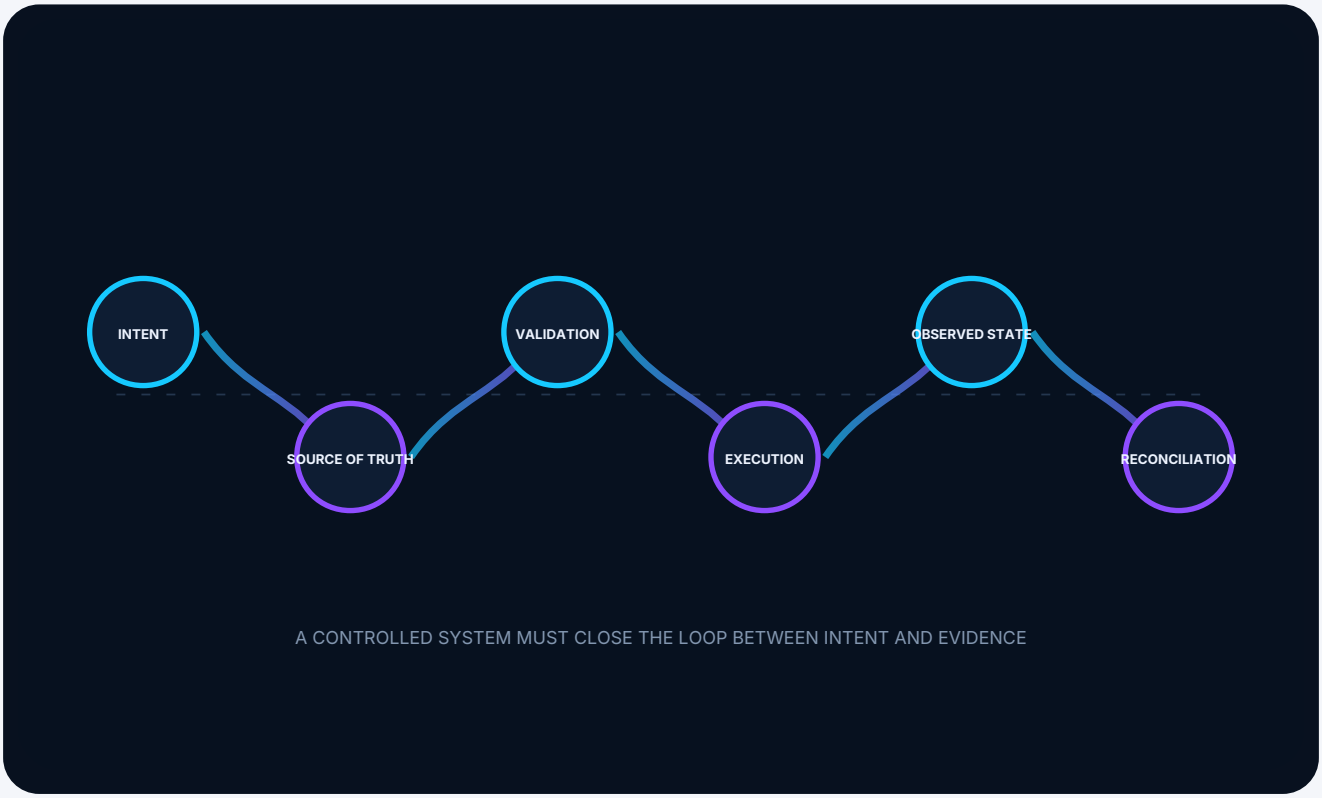
Architecture, policy, implementation, operations, and evidence are evaluated as one controlled system.

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-0001

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

Traditional evaluation of network architecture is insufficient.

Organizations measure network health by whether the monitoring dashboard is green and whether the CLI still accepts commands. They document their architecture in static Visio diagrams that are obsolete the moment they are saved. They manage their state via artisanal CLI commands passed down through tribal knowledge. This is not engineering; it is digital folklore.

This standard exists because:

1. **A Diagram is Not Architecture:** A Visio drawing is a picture, not a source of truth. It cannot be tested, verified, or reconciled. Network architecture MUST be defined as executable, version-controlled intent.
2. **CLI is Not Intent:** Typing `router bgp 65001` into a terminal is an implementation detail, not an architectural specification. Intent-Based Networking (IBN) - where the desired state is declared and the system determines the configuration - is the preferred sustainable architectural paradigm.
3. **Reachability Must Be Proven, Not Guessed:** "I think the firewall allows that flow" is an unacceptable operational posture. Network architectures MUST be mathematically verifiable. Tools like Batfish must prove reachability before a single packet is forwarded.
4. **ClickOps is high-risk architectural constraint:** Manual configuration via vendor GUIs guarantees drift, inconsistency, and outages. The network MUST be governed by Network-as-Code (NaC) and GitOps pipelines.

This document establishes the **Mythos Network Architecture Standard (MNAS)**, a comprehensive, evidence-based methodology for evaluating network architectures against intent-alignment, formal verification, and automation readiness.

ENGINEERING DOCTRINE

Part I. Scope and Applicability

1.1 In Scope

This standard covers the evaluation of:

- Network architecture topologies (Spine-Leaf, Fat-Tree, Hub-and-Spoke, Mesh)
- Intent-Based Networking (IBN) and Network-as-Code (NaC) paradigms
- Source-of-Truth (SoT) alignment (NetBox/Nautobot as authority)
- Formal verification of routing and reachability (Batfish, Forward Networks)
- Underlay and Overlay design (VXLAN/EVPN, SRv6, Segment Routing)
- Multi-vendor abstraction and normalization (OpenConfig, gNMI, YANG)
- Infrastructure-as-Code for network (Terraform, Ansible, Golden Config)
- Topology resilience, blast radius, and failure domain analysis

1.2 Out of Scope

- Specific routing protocol configurations (covered in MYTHOS-NET-0002)
- Digital twin simulation execution (covered in MYTHOS-NET-0003)
- Zero-trust network enforcement (covered in MYTHOS-SEC-0007)

1.3 Audience

- Network architects and principal engineers designing fabric topologies
- Platform engineers building Network-as-Code pipelines
- Security teams evaluating network segmentation and blast radius
- AI governance, risk, and compliance teams
- Standards bodies seeking a reference network architecture methodology

---

ENGINEERING DOCTRINE

Part II. Definitions and Taxonomy

2.1 Architecture Dimensions

Dimension	Definition
Intent-Based Networking (IBN)	A network management paradigm where the operator defines the *what* (intent) and the system determines the *how* (configuration), continuously verifying that the observed state matches the intent.
Network-as-Code (NaC)	The practice of managing network state via version-controlled, declarative code rather than imperative CLI commands.
Source-of-Truth (SoT)	The authoritative, immutable record of network intent, IP allocations, and topology (e.g., NetBox, Nautobot).
Formal Verification	The mathematical proof that a network's routing and access control tables produce the intended reachability.
Topology Drift	The divergence between the intended network architecture (SoT) and the observed state of the network devices.

2.2 The Network Architecture Doctrine

> A diagram is documentation, not truth. A CLI is implementation, not intent. A network that cannot prove its reachability is compromised. A change that is not in Git does not exist.

ENGINEERING DOCTRINE

Part III. Evaluation Methodology

3.1 Scoring Model

Each capability is scored from 0 to 5.

Score	Meaning
0	Fails basic task; CLI-driven, undocumented, unverified
1	Documented but manual, no automation or verification
2	Functional but lacks intent-alignment or formal verification
3	Solid production performance; NaC, basic verification, SoT-aligned
4	Strong performance; IBN, formal verification, SRv6/overlay abstraction
5	Best-in-class; sets the standard for autonomous, verified network architecture

Weighting

Category	Weight	Rationale
Intent-Topology Alignment & SoT	20%	Observed state must match intent or the architecture is a lie
Formal Verification & Reachability	20%	Unverified reachability is an outage waiting to happen
Network-as-Code & GitOps	15%	CLI/ClickOps guarantee drift
Topology Resilience & Blast Radius	15%	Single points of failure cause catastrophic outages
Multi-Vendor Abstraction	15%	Vendor lock-in is high-risk architectural constraint
Underlay/Overlay & SRv6 Design	10%	Modern fabrics require modern transport
Operational Lifecycle	5%	Architecture must be governed continuously

Total: 100%

A system MUST score at least 3.0 in Intent-Topology Alignment and Formal Verification to be considered for production use.

EVALUATION AND ASSURANCE SYSTEM

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

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

4.1 / CAPABILITY FAMILY

Intent-Topology Alignment and Source-of-Truth

SOURCE WEIGHT 20%

4.1.1
State Reconciliation

4.1.2
Intent Authority

MYTHOS-NET-0001-EVAL-4.1.1

State Reconciliation

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Intent-Topology Alignment and Source-of-Truth	**4.1.1**	**20%**	**Evidence-led**

Does the observed network state continuously reconcile with the Source-of-Truth?

0
No Source-of-Truth; state is whatever is on the devices

1
Static SoT (Spreadsheet/Visio) but never reconciled

2
SoT exists (NetBox) but reconciliation is manual

3
Automated periodic reconciliation with drift alerts

4
Continuous reconciliation with automated drift remediation (desired-state push)

5
Leading alignment: formally verified continuous reconciliation, policy-defined drift tolerance, and cryptographic attestation of state

ENGINEERING INTERPRETATION

This criterion evaluates whether state reconciliation 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-0001-EVAL-4.1.2

Intent Authority

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Intent-Topology Alignment and Source-of-Truth	4.1.2	20%	Evidence-led

Is the SoT the designated authority for network intent?

0
Devices are the source of truth; changes made directly

1
SoT exists but out-of-band changes are common

2
SoT is authoritative but not enforced (drift accepted)

3
SoT is enforced; out-of-band changes trigger alerts and are overwritten

4
SoT is enforced via GitOps; all changes require PR and CI/CD pipeline

5
Leading authority: immutable SoT, zero out-of-band change capability, cryptographic signing of intent

ENGINEERING INTERPRETATION

This criterion evaluates whether intent authority 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.

4.2 / CAPABILITY FAMILY

Formal Verification and Reachability

SOURCE WEIGHT 20%

4.2.1
Reachability Proof

4.2.2
Intent Verification

MYTHOS-NET-0001-EVAL-4.2.1

Reachability Proof

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Formal Verification and Reachability	**4.2.1**	**20%**	**Evidence-led**

Can the architecture mathematically prove its reachability?

0
No verification; reachability tested via ping/traceroute in production

1
Manual peer review of configurations

2
Automated syntax/semantic validation (linting)

3
Pre-deployment simulation (Batfish) for major changes

4
Continuous formal verification of all routing and ACL tables

5
Leading verification: mathematically proven reachability invariants, continuously verified in CI/CD, and cryptographically sealed topology maps

ENGINEERING INTERPRETATION

This criterion evaluates whether reachability proof 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-0001-EVAL-4.2.2

Intent Verification

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Formal Verification and Reachability	**4.2.2**	**20%**	**Evidence-led**

Does the system verify that the deployed configuration actually fulfills the architectural intent?

0
No verification; hope the config works

1
Post-deployment manual testing

2
Automated post-deployment ping/ connectivity checks

3
Automated configuration compliance (Greenbone/NetMRI)

4
Formal intent verification (Batfish assertion: "Can A reach B on port 443?")

5
Leading verification: continuous intent assertion, automated rollback on violation, and mathematical proof of policy compliance

ENGINEERING INTERPRETATION

This criterion evaluates whether intent verification 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

Network-as-Code and GitOps

SOURCE WEIGHT 15%

4.3.1
Configuration Generation

4.3.2
Change Control

MYTHOS-NET-0001-EVAL-4.3.1

Configuration Generation

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Network-as-Code and GitOps	**4.3.1**	**15%**	**Evidence-led**

How is network configuration generated and deployed?

0
Manual CLI commands

1
Copy-paste templates

2
Scripts generating configs but not applied via pipeline

3
Infrastructure-as-Code (Terraform/ Ansible) via CI/CD

4
GitOps pull-model (ArgoCD/Flux reconciling network state)

5
Leading NaC: intent-driven generation, GitOps reconciliation, automated diff, and zero human CLI access

ENGINEERING INTERPRETATION

This criterion evaluates whether configuration generation 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-0001-EVAL-4.3.2

Change Control

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Network-as-Code and GitOps	4.3.2	15%	Evidence-led

Are all network changes version-controlled and peer-reviewed?

0
No version control; changes made ad-hoc

1
Backups saved to a shared drive

2
Git repository exists but not used for all changes

3
All changes require PR and peer review before merge

4
PR triggers CI pipeline (lint, simulate, verify) before merge

5
Leading control: PR, CI verification, formal proof, automated deploy, and cryptographic audit trail

ENGINEERING INTERPRETATION

This criterion evaluates whether change control 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.

4.4 / CAPABILITY FAMILY

Topology Resilience and Blast Radius

SOURCE WEIGHT 15%

4.4.1
Failure Domain Isolation

4.4.2
Redundancy Verification

MYTHOS-NET-0001-EVAL-4.4.1

Failure Domain Isolation

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Topology Resilience and Blast Radius	**4.4.1**	**15%**	**Evidence-led**

Are failure domains minimized and isolated?

0
Flat network; single failure domain

1
Basic hierarchy but no fault isolation

2
Modular design (Spine-Leaf) but shared control plane

3
Isolated failure domains with independent control planes

4
Blast radius bounded by topology; automated failover verified by twin

5
Leading resilience: formally verified blast radius limits, sub-second convergence, and self-healing paths

ENGINEERING INTERPRETATION

This criterion evaluates whether failure domain 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

- 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-0001-EVAL-4.4.2

Redundancy Verification

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Topology Resilience and Blast Radius	**4.4.2**	**15%**	**Evidence-led**

Is redundancy mathematically verified, not just designed?

0
No redundancy

1
Dual hardware but untested failover

2
Manual failover testing annually

3
Automated failover testing (chaos engineering)

4
Continuous verification of redundant paths via digital twin

5
Leading verification: formally proven N+1/N+2 redundancy, continuous path validation, and zero single points of failure

ENGINEERING INTERPRETATION

This criterion evaluates whether redundancy verification 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

Multi-Vendor Abstraction

SOURCE WEIGHT 15%

4.5.1
Vendor Neutrality

MYTHOS-NET-0001-EVAL-4.5.1

Vendor Neutrality

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Multi-Vendor Abstraction	**4.5.1**	**15%**	**Evidence-led**

Is the architecture abstracted from vendor-specific CLI/dependencies?

0
Single vendor lock-in; proprietary CLI only

1
Multi-vendor but separate silos per vendor

2
Multi-vendor with standardized data models (OpenConfig/YANG)

3
Unified abstraction layer (gNMI/ RESTCONF) over multi-vendor

4
Intent-driven abstraction; vendor config is a derived artifact

5
Leading abstraction: trait-based interfaces, zero vendor-specific logic in intent, automated conformance testing

ENGINEERING INTERPRETATION

This criterion evaluates whether vendor neutrality 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

Underlay/Overlay and SRv6 Design

SOURCE WEIGHT 10%

4.6.1
Transport Architecture

MYTHOS-NET-0001-EVAL-4.6.1

Transport Architecture

FAMILY	SOURCE REFERENCE	WEIGHT CONTEXT	ASSESSMENT POSTURE
Underlay/Overlay and SRv6 Design	4.6.1	10%	Evidence-led

Does the architecture use modern, programmable transport?

0
Legacy VLAN-based flat transport

1
MPLS/LDP or VXLAN with manual BGP EVPN

2
Automated VXLAN/EVPN fabric

3
SR-MPLS or SRv6 underlay with automated provisioning

4
SRv6 with programmable SIDs (traffic engineering, SLA)

5
Leading transport: SRv6, automated TE, formally verified path computation, and AI-driven optimization

ENGINEERING INTERPRETATION

This criterion evaluates whether transport 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.

LIFECYCLE AND ASSURANCE

Part V. The Mythos Network Architecture Suite (MNAS)

Traditional network benchmarks measure convergence time. The MNAS evaluates intent alignment, formal verification, and resilience.

5.1 Suite Composition

5.1.1 MNAS-Intent

- **Drift Detection:** 100+ tests injecting out-of-band changes to verify they are detected and overwritten.
- **SoT Authority:** 50+ tests verifying no device configuration exists that is not derived from the SoT.

5.1.2 MNAS-Verification

- **Reachability Assertions:** 100+ Batfish assertions verifying critical flows (e.g., "Web tier cannot reach DB tier on port 22").
- **Failover Verification:** 50+ tests simulating link/node failures in the digital twin to verify path redundancy.

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.