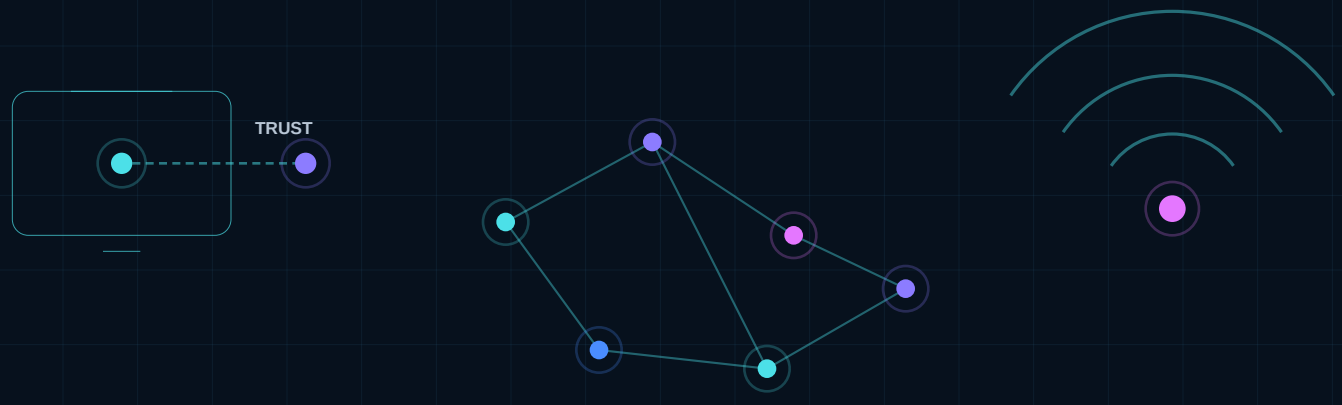
MYTHOS SYSTEMS

ENGINEERING GUIDE

Endpoint, Edge, OT, IoT, and Telecommunications Operations Guide

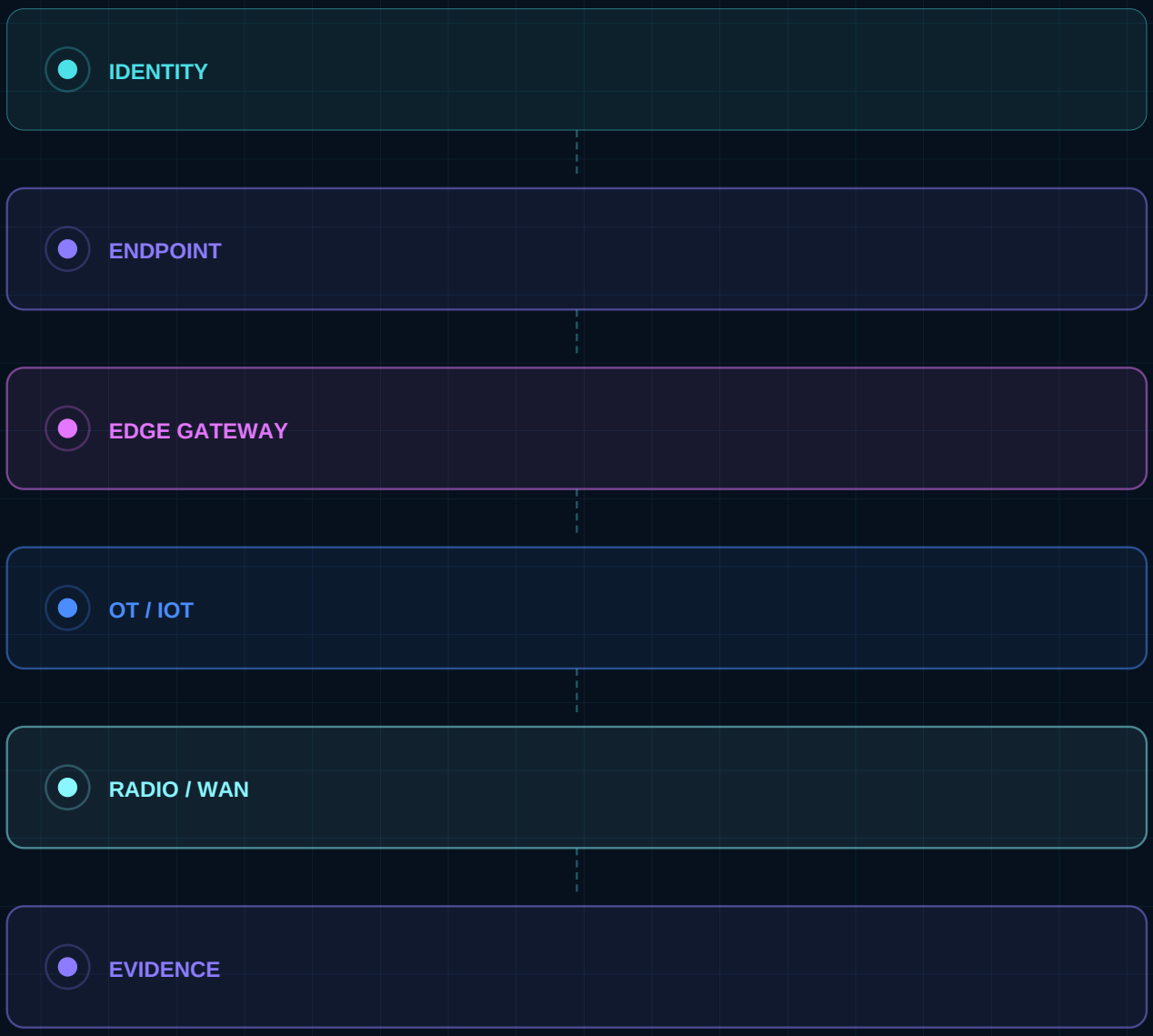
Operational integration across endpoint trust, industrial zones, edge fleets, sensors, radio systems, remote access, and lifecycle assurance.



MYTHOS-GUIDE-EDGE-0001

PERMANENT PUBLICATION IDENTITY / CANDIDATE PUBLICATION / PUBLIC

Operating architecture



Evidence-bearing implementation path

01 DEFINE SCOPE & AUTHORITY

02 MODEL STATE & BOUNDARIES

03 IMPLEMENT POLICY & AUTOMATION

04 OBSERVE REAL EFFECTS

05 TEST FAILURE & RECOVERY

06 RECONCILE EVIDENCE

The guide remains informative; conformance is established only by the applicable permanent standards and evidence.

INFRASTRUCTURE AND CONTROL TOPOLOGY

Operational Technology and Critical Infrastructure

A trustworthy endpoint, ot, telecom, and iot engineering guide system is a governed chain of ownership, identity, desired state, enforcement, workload or device behavior, telemetry, recovery, and independently reviewable evidence.

OWNERSHIP

Purpose, service boundary, accountable owner, suppliers, users, and retained responsibility remain explicit.

ENFORCEMENT

Identity, policy, segmentation, configuration, and local safety mechanisms constrain every trust transition.

CONTINUITY

Capacity, dependency loss, safe degradation, backup, restoration, rollback, and exit are tested before reliance.

EVIDENCE

Inventory, desired state, runtime observation, tests, incidents, exceptions, and change records form the assurance chain.

GOVERNED INFRASTRUCTURE FLOW

Reconciliation, detection, response, restoration, and controlled evolution

INTERPRETATION AND ASSURANCE

How to apply this publication

Normative intent

Requirements define outcomes and constraints. Implementations may vary, but evidence must demonstrate equivalent control.

Evidence over assertion

Vendor documentation and design intent are not equivalent to reproduced behavior. Record evidence grade and uncertainty.

Risk-proportional depth

Higher consequence, autonomy, sensitivity, and irreversibility require stronger isolation, review, verification, and recovery.

Controlled exception

Exceptions require an owner, rationale, compensating control, residual-risk acceptance, expiration, and reevaluation trigger.

Normalized assessment scale

0	1	2	3	4	5
ABSENT	AD HOC	PARTIAL	OPERATIONAL	ADVANCED	LEADING

A numeric score must never hide a failed mandatory gate, missing evidence, untested workload, or unacceptable residual risk.

MYTHOS-GUIDE-EDGE-0001 / OPERATIONAL TECHNOLOGY

Engineering Doctrine

Cross-domain guide for managed endpoints, cyber-physical systems, mobile and indoor RF, telephony, IoT, and disco

OPERATING POSITION

Start from mission, process, safety, communications, identity, and lifecycle consequences.

- Use local enforcement and safe degradation where cloud or management dependencies cannot be assumed.

MYTHOS-GUIDE-EDGE-0001 / OPERATIONAL TECHNOLOGY

Device Lifecycle

OPERATING POSITION

Bind procurement or manufacture, identity, commissioning, configuration, software, posture, data, support, transfer, reset, and retirement.

MYTHOS-GUIDE-EDGE-0001 / OPERATIONAL TECHNOLOGY

OT Change and Recovery

OPERATING POSITION

Use process ownership, hazard review, passive observation, versioned golden state, maintenance windows, rollback, and process validation.

MYTHOS-GUIDE-EDGE-0001 / OPERATIONAL TECHNOLOGY

Telecom and Radio

OPERATING POSITION

Correlate identity, signaling, user plane, radio, timing, QoS, emergency obligations, carriers, power, and service quality.

MYTHOS-GUIDE-EDGE-0001 / OPERATIONAL TECHNOLOGY

Field Evidence

OPERATING POSITION

Preserve as-built design, coverage, device, firmware, session, process, recovery, consent, safety, and authority records.

MYTHOS-GUIDE-EDGE-0001 / OPERATIONAL TECHNOLOGY

Publication Controls and Decision Record

Permanent identity, evidence, exceptions, and revision discipline

- Document identity remains stable across revision and packaging.
- Evidence grades and uncertainty accompany consequential claims.
- Exceptions are time-bounded and independently visible.
- Source currency is reviewed at assessment and scheduled publication review.
- Release artifacts are hashed and listed in the public manifest.

MYTHOS-GUIDE-EDGE-0001

MYTHOS SYSTEMS / ENGINEERING STANDARDS LIBRARY

MYTHOS-GUIDE-EDGE-0001 / OPERATIONAL TECHNOLOGY

Publication Controls and Decision Record

Permanent identity, evidence, exceptions, and revision discipline

- Document identity remains stable across revision and packaging.
- Evidence grades and uncertainty accompany consequential claims.
- Exceptions are time-bounded and independently visible.
- Source currency is reviewed at assessment and scheduled publication review.
- Release artifacts are hashed and listed in the public manifest.

MYTHOS-GUIDE-EDGE-0001

MYTHOS SYSTEMS / ENGINEERING STANDARDS LIBRARY

MYTHOS-GUIDE-EDGE-0001 / OPERATIONAL TECHNOLOGY

Publication Controls and Decision Record

Permanent identity, evidence, exceptions, and revision discipline

- Document identity remains stable across revision and packaging.
- Evidence grades and uncertainty accompany consequential claims.
- Exceptions are time-bounded and independently visible.
- Source currency is reviewed at assessment and scheduled publication review.
- Release artifacts are hashed and listed in the public manifest.

MYTHOS-GUIDE-EDGE-0001

MYTHOS SYSTEMS / ENGINEERING STANDARDS LIBRARY

MYTHOS-GUIDE-EDGE-0001 / OPERATIONAL TECHNOLOGY

Publication Controls and Decision Record

Permanent identity, evidence, exceptions, and revision discipline

- Document identity remains stable across revision and packaging.
- Evidence grades and uncertainty accompany consequential claims.
- Exceptions are time-bounded and independently visible.
- Source currency is reviewed at assessment and scheduled publication review.
- Release artifacts are hashed and listed in the public manifest.

MYTHOS-GUIDE-EDGE-0001

MYTHOS SYSTEMS / ENGINEERING STANDARDS LIBRARY

MYTHOS-GUIDE-EDGE-0001 / OPERATIONAL TECHNOLOGY

11. Source Authority and Reference Register

Primary sources informing interpretation; current obligations and provider behavior must be verified at assessment t

NIST CSF 2.0 — **Cybersecurity Framework 2.0**

https://doi.org/10.6028/NIST.CSWP.29

Enterprise governance and cybersecurity outcome framework.

NIST SP 800-53 Rev. 5 — **Security and Privacy Controls for Information Systems and Organizations**

https://doi.org/10.6028/NIST.SP.800-53r5

Broad control baseline for organizational systems and services.

NIST SP 800-82 Rev. 3 — **Guide to Operational Technology Security**

https://doi.org/10.6028/NIST.SP.800-82r3

OT architecture, threats, controls, safety context, and lifecycle guidance.

IEC 62443 Series — **Security for industrial automation and control systems**

https://www.iec.ch/industrial-cyber-security

Industrial security lifecycle, zones, conduits, and component requirements.

MITRE ATT&CK for ICS — **ATT&CK for Industrial Control Systems**

https://attack.mitre.org/matrices/ics/

Adversary behavior and technique knowledge base for ICS.

CISA ICS — **Industrial Control Systems Cybersecurity Guidance**

https://www.cisa.gov/topics/industrial-control-systems

Operational advisories, practices, and incident resources.

Source currency rule: authorities, specifications, legal obligations, provider services, firmware, browser behavior, carrier requirements, and operational evidence MUST be checked at assessment time. This publication records a 2026-07-24 source snapshot.