

Mode-Aware Object-Level Security for EtherNet/IP Devices Using CIP Security in Industrial Network

Technical Paper Presentation

ODVA 2026 Industry Conference & 24th Annual Meeting

Shyam Sundar Pal, Firmware Architect
Riya Rahul Shah, Senior Functional Safety Lead
Utthunga Technologies, India

October 21, 2026

Presentation Outline

- Motivation: endpoint authorization after CIP Security / (D)TLS
- Problem: network and transport controls do not validate every CIP command
- Solution: fail-closed L1–L4 enforcement pipeline on the device
- Standards: composition with ODVA CIP Security Volume 8
- Deployment: feasibility, cost-benefit, and differentiation

*Here L1-L4 provides different **levels** not any specific network **layers***

2026 ODVA
Industry Conference and Annual Meeting

Background & Motivation

Why Device Security Matters

- IT/OT convergence exposes industrial devices to broader networks
- Firewalls, segmentation, VPN, and TLS secure the path—not every CIP operation at the endpoint
- CIP Security provides authenticated transport; gap remains object-level authorization and mode-aware control
- Scope (paper): endpoint enforcement extension—no new transport or replacement of CIP Security profiles
- Devices must defend themselves, not rely on the perimeter alone

Abstract

- Challenge: securing industrial devices when network controls are bypassed
- Scope: device-local policy after CIP Security—session binding, operational-mode validation, CIP object/service ACL
- Problem: encrypted or accepted sessions can still carry unauthorized CIP commands
- Approach: sequential post-(D)TLS checks with shared policy context and fail-closed rejection
- Contribution: practical composition toward Authorization Profile direction using mutual agreement and mode-aware gates



Problem Statement

Network Security Is Not Sufficient

- Perimeter controls cannot guarantee valid CIP operations on the device
- Encrypted channels may still carry unauthorized CIP commands
- IDS often detects after frames are accepted—prevention requires inline device policy
- CIP Security addresses transport; this work addresses endpoint authorization after transport is established

Four Failure Modes

- Encrypted malicious payload inside a valid TLS/VPN tunnel
- Detection without prevention at the device
- No end-to-end command trust at the protocol layer
- Stateful process abuse against current operational mode

1 Encrypted malicious payload
The channel is secure, but the CIP command may still be unauthorized for this requester.

2 Detection without prevention
IDS / NIDS raise alerts but typically do not block execution inside the device.

3 No end-to-end command trust
Network ACLs do not validate CIP object, attribute and service permissions.

4 Stateful process abuse
Authenticated requester issues an operation that is wrong for the current device mode.

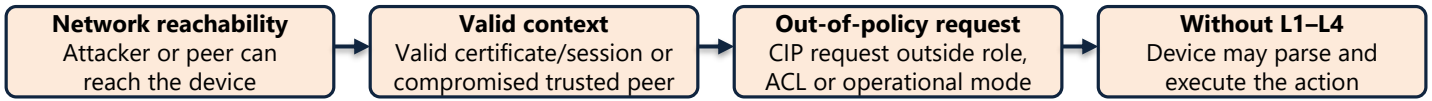
Proposed: L1–L4 Device Policy Engine after CIP Security
Header-first · session binding · mode-aware gate · object ACL · fail-closed

Gaps in Existing Approaches

- Insufficient device-layer authentication and command validation
- IDS monitors EtherNet/IP traffic but does not block execution
- Packets can be accepted and processed even when unauthorized
- Real-time OT environments need inline prevention, not alerts alone

Problem Statement & Impact

- Need: device-integrated, header-first inspection with session, mode, and object policy
- Principles: fail-closed, least privilege, state-aware context, mutual agreement on object access
- Impact if unresolved: malicious config/firmware, session/state abuse, lateral exposure, IEC 62443 least-privilege gaps



In scope (this paper)
- Post-(D)TLS per-request policy
- Session binding and object/service ACL
- Operational-mode authorization
- Fail-closed rejection

Out of scope
- New transport or cryptography
- Redefining the Authorization Profile



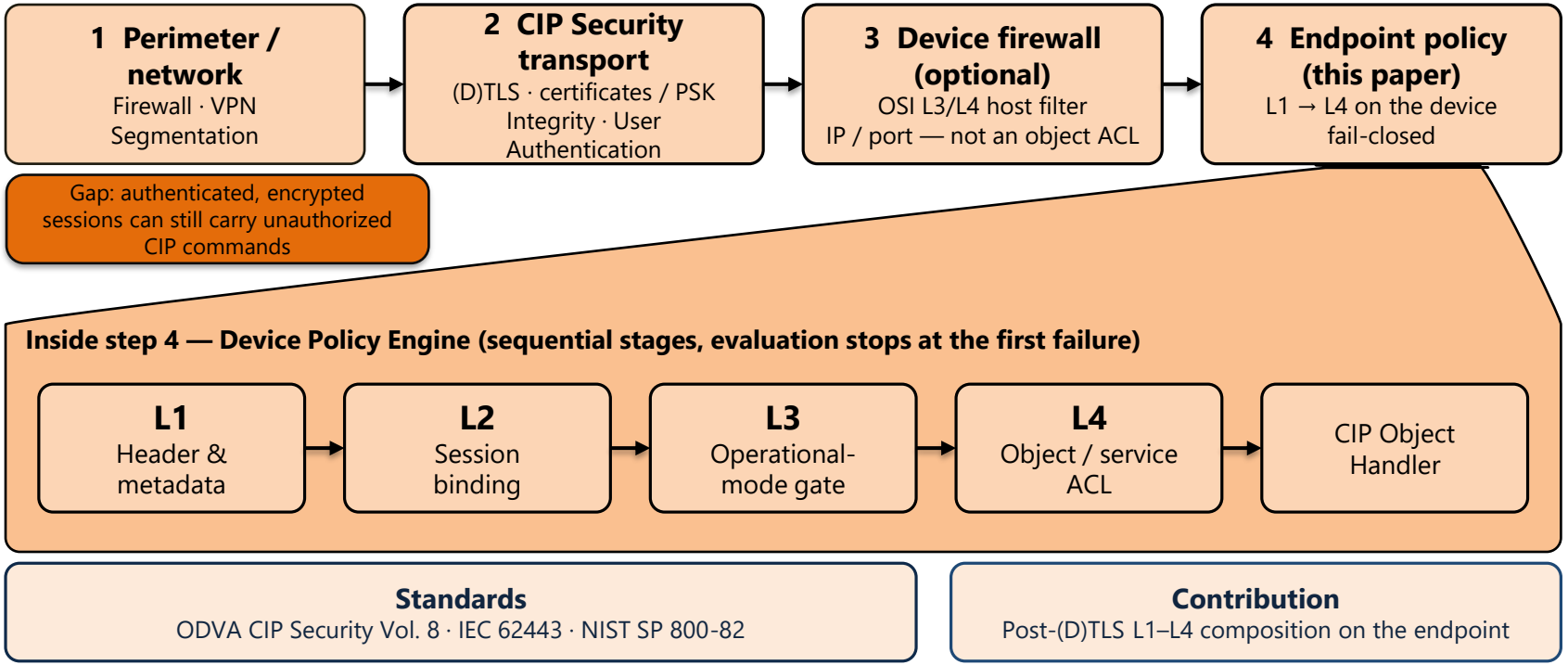
Proposed Architecture

Solution Overview

- Endpoint enforcement on the EtherNet/IP device after CIP Security transport is established
- Sequential L1–L4 application-policy checks—not four independent authorization engines
- One shared policy store; evaluation stops at the first failed stage
- Device-based firewall may filter traffic but does not replace L1–L4 CIP policy
- Complements network security; does not replace it

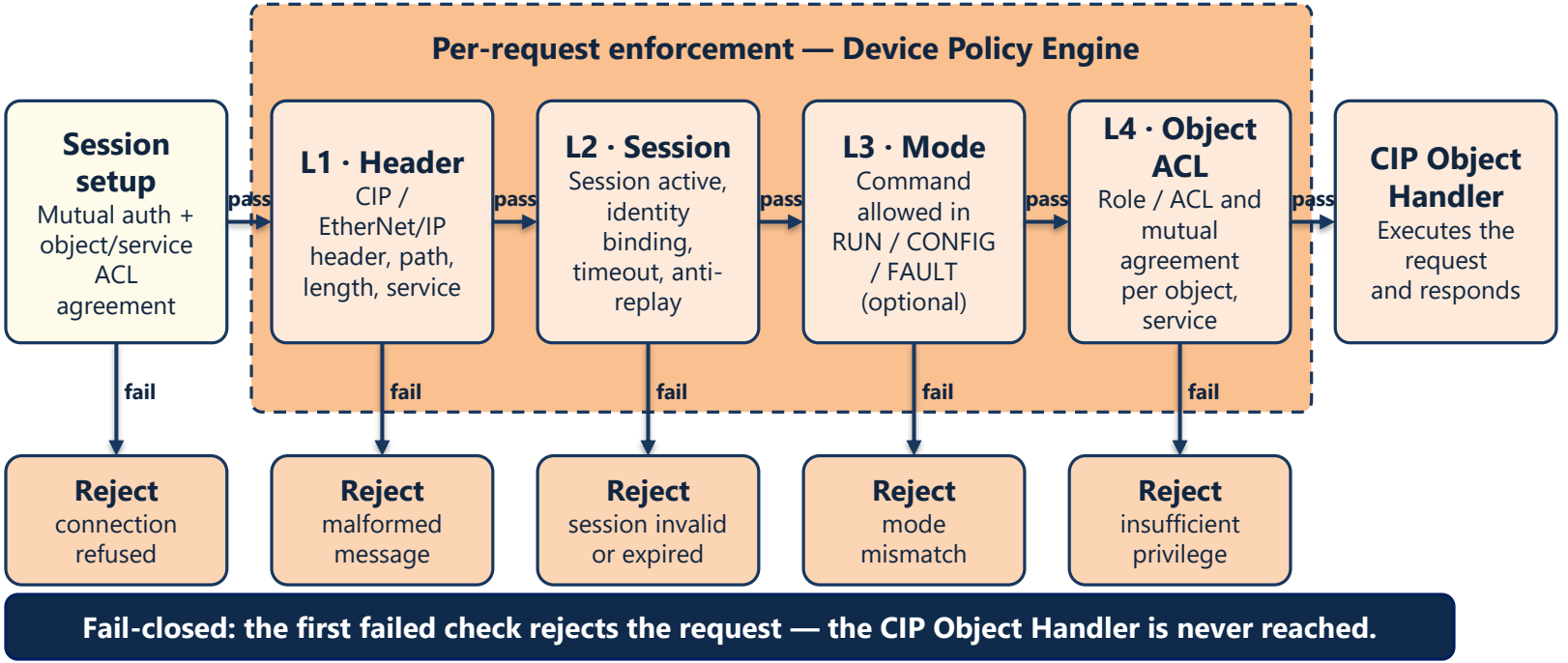
Approach	What it secures	Endpoint CIP control?
Firewall / segmentation	Network zones and paths	No — no object-level ACL
CIP Security transport	Channel auth, integrity, confidentiality	Partial — object policy still needed
EtherNet/IP IDS	Traffic anomaly detection	Detects — not an inline block
Proposed Solution— L1–L4	**Session, Mode, object & service ACL**	**Yes — fail-closed before handler**

Endpoint Policy Enforcement



© 2026 ODVA, Inc.
All rights reserved.

Per-Request Endpoint Enforcement

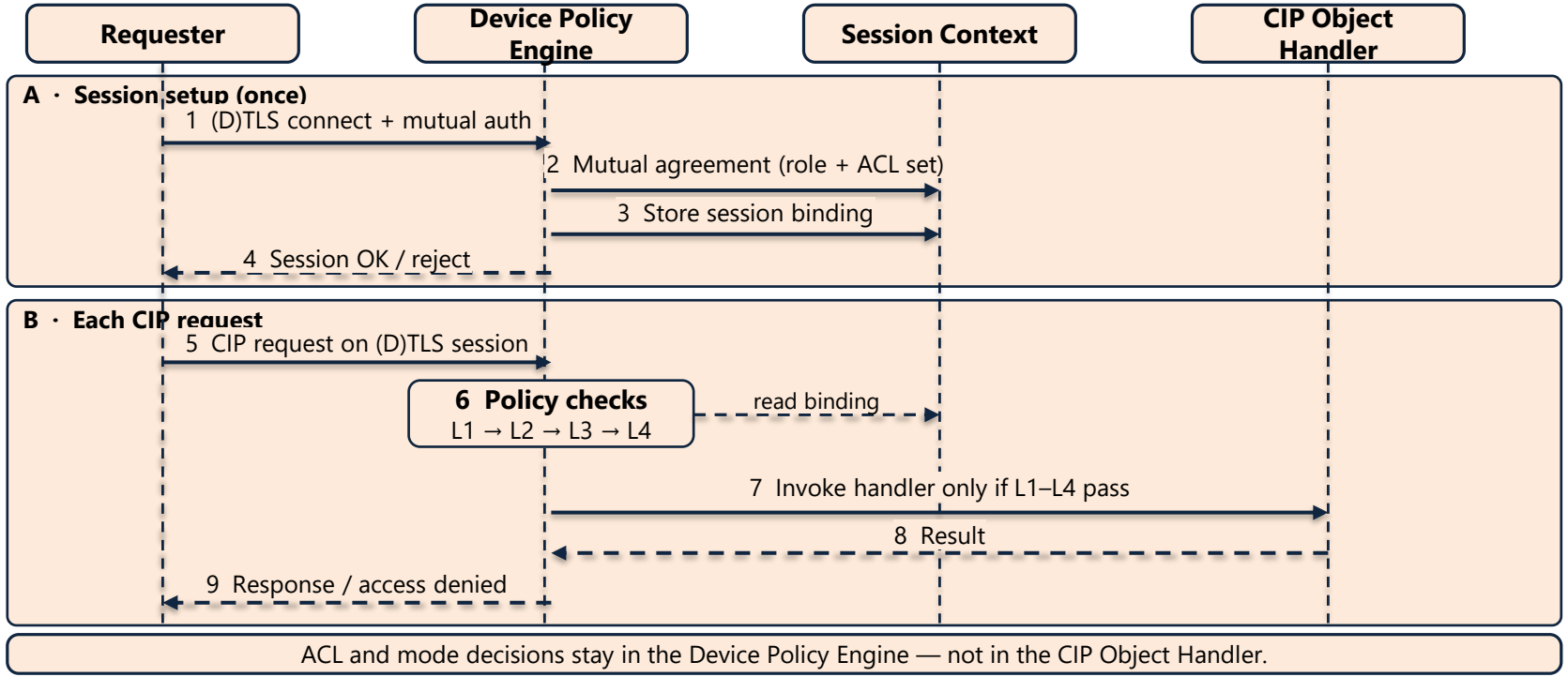


L1–L4 are sequential stages of one policy engine, not OSI layers

© 2026 ODVA, Inc.

All rights reserved.

Requester ↔ Device Policy Engine ↔ CIP Handler



© 2026 ODVA, Inc.

All rights reserved.



Level Details Flow (L1–L4)

L1 — Header and Metadata Inspection

- Inspect EtherNet/IP encapsulation and CIP header fields only
- Validate structure, length, service code, path, and sequence
- Reject malformed CIP messages; extract context for later ACL
- Not Device-Based Firewall; not by itself an object allow/deny

L2 — Session Binding per Requester

- Bind authenticated identity/role to session context on every request
- User Authentication Session ID is distinct from TLS/DTLS transport identifiers
- Validate session active, keys/tokens, timeout, anti-replay, and source identity
- Failure: session not found, mismatch, expired, or invalid binding

L3 — Operational-Mode Gate

- Verify requested CIP service is allowed in current device mode (Running, Config, Fault, etc.)
- Formalizes mode-aware authorization—does not replace the device state machine
- Many vendors already restrict writes by mode; this stage composes that into endpoint policy
- Related to CIP Security Object commissioning/state—not a duplicate safety PLC logic

L4 — CIP Object or Service Authorization

- Evaluate CIP class/instance/attribute/service against role and ACL
- Object-level mutual agreement at session setup—toward Authorization Profile direction
- Practical endpoint enforcement; does not redefine ODVA Authorization Profile specification
- Failure: access denied / insufficient privilege (fail-closed)

2026 ODVA
Industry Conference and Annual Meeting

Standards & Differentiation

Alignment with ODVA CIP Security

- Built on Volume 8: TLS/DTLS, X.509, HMAC, security objects
- Composes Confidentiality, User Authentication, Device-Based Firewall
- Object-level mutual agreement anticipates Authorization Profile direction
- Mutual agreement is proposed endpoint policy — not a standardized Authorization Profile handshake
- Operational-mode gating similarly remains an application-layer extension

How We Differ from Prior Approaches

- Firewall/segmentation: network filter, no CIP command legitimacy at endpoint
- VPN/TLS/CIP Security transport: secures channel; object-level policy still required
- IDS: detection outside device processing path

- *This paper: post-(D)TLS fail-closed composition of session, mode, and object policy*

Device-Based Firewall vs CIP Object Policy

- Device-Based Firewall: OSI L3/L4 host filter (IP, port, protocol)—existing CIP Security profile
- CIP object/service ACL: post-(D)TLS application authorization on the endpoint
- Object-level mutual agreement: practical policy toward Authorization Profile direction
- Pipeline L3/L4 ≠ OSI L3/L4 firewall—naming is enforcement stage vs network layer

2026 ODVA
Industry Conference and Annual Meeting

Conclusion

Key Takeaways

- Network and transport security are necessary but insufficient for EtherNet/IP endpoints
- Devices need header-first, sequential L1–L4 inline prevention after CIP Security
- Proposal composes with Volume 8—extends with mode-aware, object-level endpoint enforcement
- Best value where distinct object permissions, session-scoped auth, or mode-aware control matter
- Single-level authorization may suffice for simple devices; pipeline adds structure when policy composes

Thank You

- Questions and Discussion
- Shyam Sundar Pal | Riya Rahul Shah, Utthunga Technologies, India
- Contact us after the session for technical follow-up

- *ODVA 2026 Industry Conference | www.odva.org*