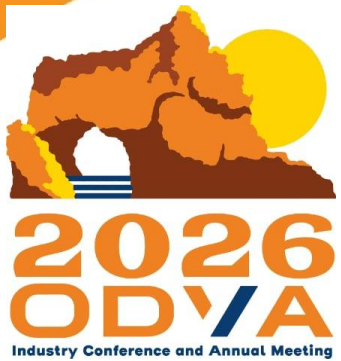


Redefining Industrial Networks

From Topology to Interaction

Rob Lodesky
Director of Strategic Accounts
HMS Industrial Networks
October 21, 2026

What You Will Learn

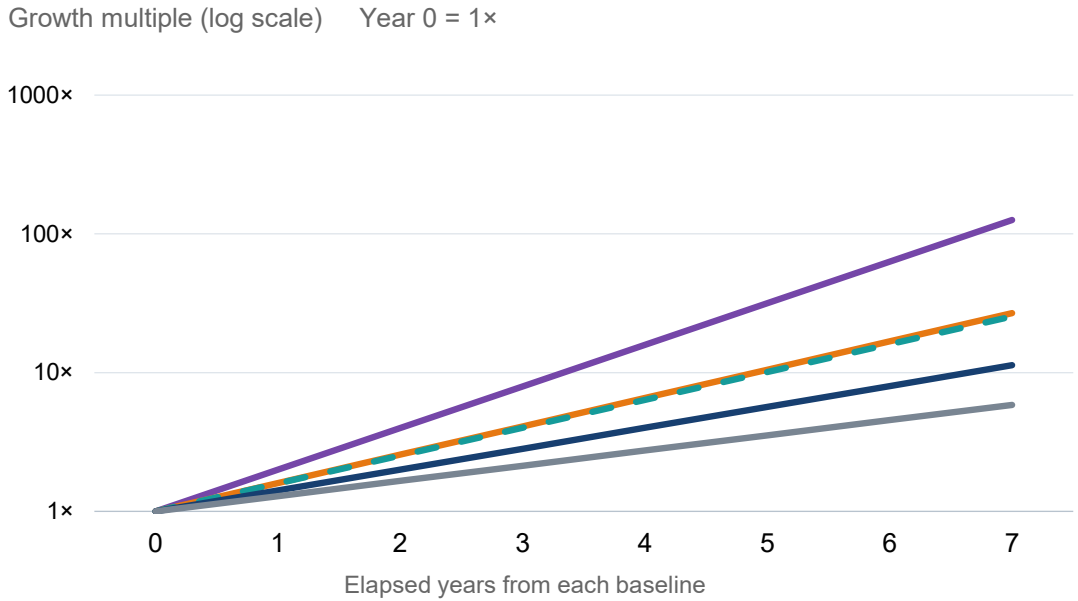
Three ways to see, test, and improve industrial networks.

 © 2026 ODVA, Inc.

All rights reserved.

IoT data, AI compute, bandwidth and chip scaling

Normalized growth comparison: same starting index, different underlying metrics



Huang's law [1]
AI inference: 1,000× / decade*
≈1.00 yr doubling; 125.9× at year 7

Industrial / automotive IoT [2]
Generated data: 60% CAGR
1.47 yr doubling; 26.8× at year 7

Edholm's law [3]
Bandwidth: 2× / 18 months
1.50 yr doubling; 25.4× at year 7

Moore's law [4]
Transistor count: 2× / 2 years
2.00 yr doubling; 11.3× at year 7

Total IoT data [2]
Generated data: 28.7% CAGR
2.75 yr doubling; 5.85× at year 7

IoT model: $D(t) = D_0(1 + r)^t$. IDC's 2019 forecast covered 2018–2025; it is not a universal ingestion law.

Constant-rate equivalents, not measured trajectories or verified 2025 outcomes. *Huang curve uses NVIDIA's 2023 retrospective claim, not a fixed universal rate. Sources: [1] NVIDIA (2023) [2] IDC via Help Net Security / FutureIoT (2019) [3] IEEE Spectrum (2004), Edholm summary [4] Our World in Data (2023).

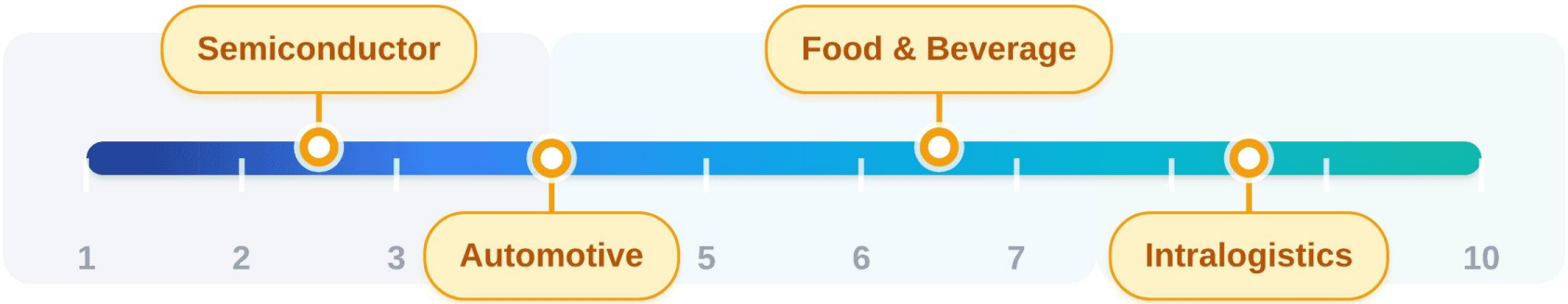
Hierarchical Distributed Intelligence Architecture

COMPLETELY CENTRALIZED

Single orchestration point for all decisions

COMPLETELY DECENTRALIZED

Fully autonomous nodes with multiple hubs



Where does CIP fit?

Democratic Route

What other intelligent models can we think of to study?

Why Borrow From Other Fields?

9.2-to-1

Social-network research dwarfs industrial-network research.

Borrow adjacent ideas carefully.

More Capability Creates More Behavior

Edge compute and IoT growth create **more interaction behavior** to govern, not just more data.

When Devices Start to Reason

What should humans specify?

What should agents discover?

The agentic co-design question.

Social-network heuristics help interpret interaction

As devices gain agency, engineers must understand the relationships they create.

Humans specify purpose, permitted behavior and operating limits.

Agents can help discover interaction patterns within those constraints.

PATTERN TO INVESTIGATE	SOCIAL-NETWORK LENS	INDUSTRIAL QUESTION
Repeated local exchanges	Triadic closure and modularity	Where do functional clusters emerge?
Growing reliance on a few nodes	Preferential attachment and centrality	Which hubs concentrate dependency?
Links between separate groups	Brokerage and structural holes	Which crossings carry critical coordination?

Borrow the analytical lens, then validate the industrial behavior.

These heuristics guide investigation. They do not establish timing, safety or security guarantees.

Heuristic 1: Triadic Closure

WHAT IT EXPLAINS

Repeated interactions naturally thicken into dense local clusters.

NETWORK VALUE

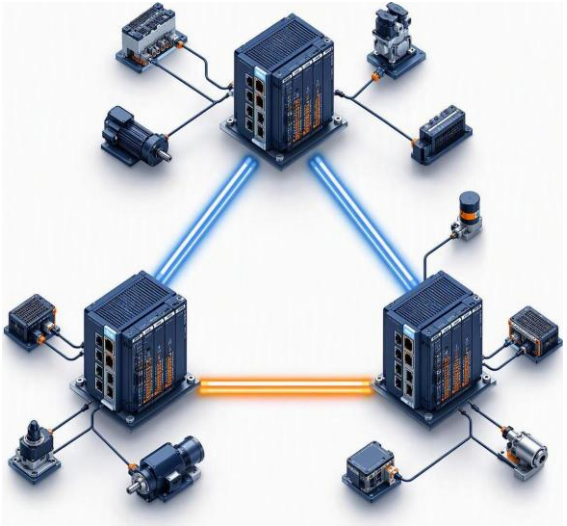
Builds localized resilience, redundancy, and structural trust.

INDUSTRIAL RELATION

Maps to device-level subnets and implicit operational zones.

AI POTENTIAL

Agents can auto-detect hidden interaction clusters to suggest optimal segmentation boundaries.



Heuristic 2: Preferential Attachment

WHAT IT EXPLAINS

High-capacity hubs naturally attract a disproportionate share of new links over time.

NETWORK VALUE

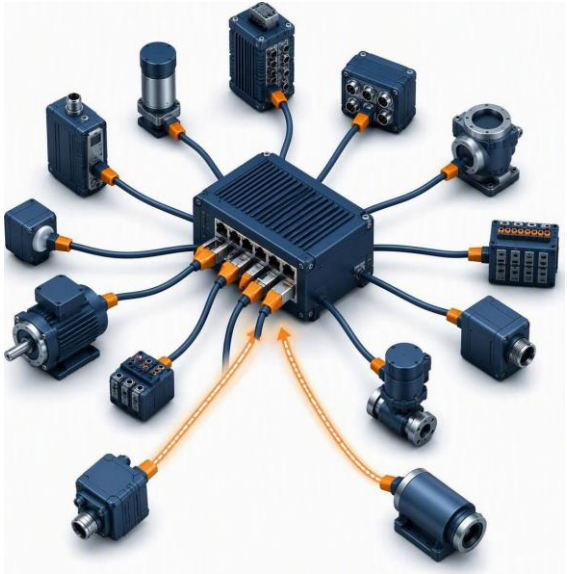
Creates highly efficient routing, discoverability, and resource centralization.

INDUSTRIAL RELATION

Explains controller consolidation, main gateway bottlenecks, and centralized historian servers.

AI POTENTIAL

Agents can forecast chokepoint formation before a hub exceeds its logical or physical limits.



Heuristic 3: Betweenness Centrality

WHAT IT EXPLAINS

Nodes on the shortest paths between other nodes act as critical coordinators or bottlenecks.

NETWORK VALUE

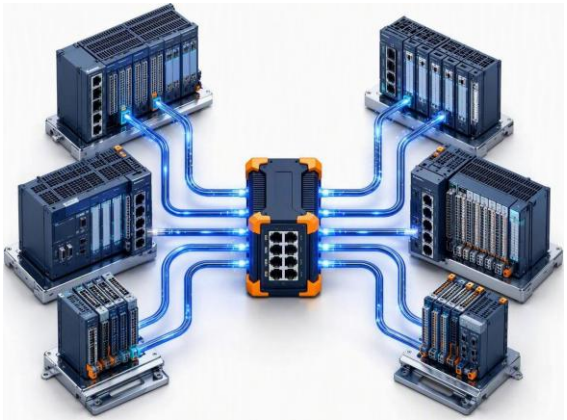
Minimizes hop counts and accelerates global state synchronization across the system.

INDUSTRIAL RELATION

Defines the vulnerability of core switches, backbone links, and inter-zone firewalls.

AI POTENTIAL

Agents can dynamically reroute non-critical traffic away from high-centrality nodes during operational spikes.



Heuristic 4: Modularity

WHAT IT EXPLAINS

Networks organize into dense internal clusters connected by sparse external bridges.

NETWORK VALUE

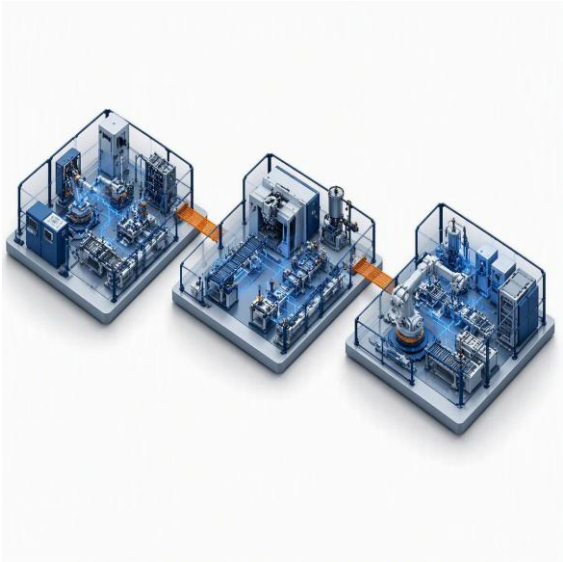
Localizes traffic, contains cascading faults, and creates natural security boundaries.

INDUSTRIAL RELATION

Maps directly to cell/area zones, VLANs, and physical plant segmentation strategies.

AI POTENTIAL

Agents can suggest boundary updates by observing where cross-cluster traffic naturally shifts over time.



Heuristic 5: Brokerage

WHAT IT EXPLAINS

Nodes that bridge structural holes control the flow between otherwise disconnected groups.

NETWORK VALUE

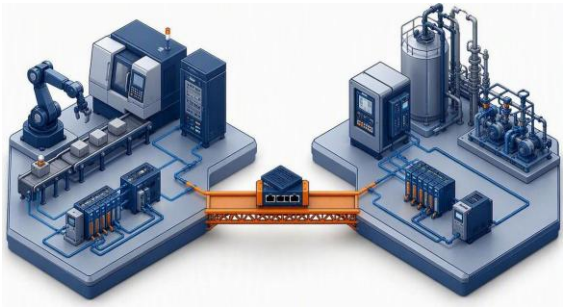
Enables targeted cross-domain coordination without flooding the entire network.

INDUSTRIAL RELATION

Explains the critical role of IT/OT gateways, DMZ servers, and cross-cell data brokers.

AI POTENTIAL

Agents can dynamically provision or revoke brokerage access based on real-time operational context.



Heuristic 6: Information Cascades

WHAT IT EXPLAINS

Hub effects amplify both growth and failure nonlinearly across the entire system.

NETWORK VALUE

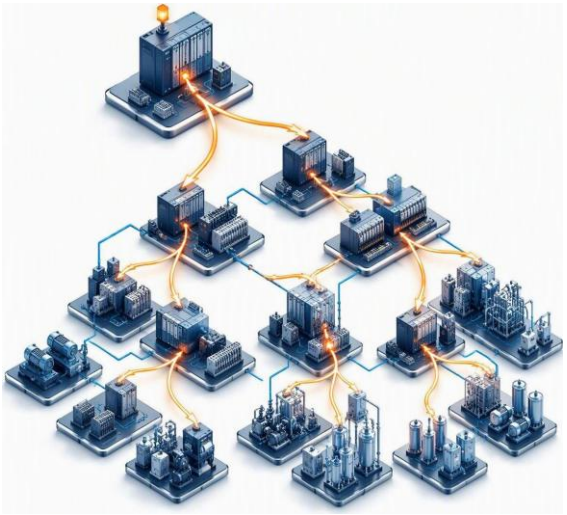
Explains how small initial triggers can produce massive, rapid systemic shifts.

INDUSTRIAL RELATION

Underlies broadcast storms, synchronized reboot failures, and cascading alarm floods.

AI POTENTIAL

Agents can model cascade thresholds to automatically halt traffic that risks triggering a storm.



Heuristic 7: K-Core Decomposition

WHAT IT EXPLAINS

Tie redundancy maps directly to the systemic resilience of the network core.

NETWORK VALUE

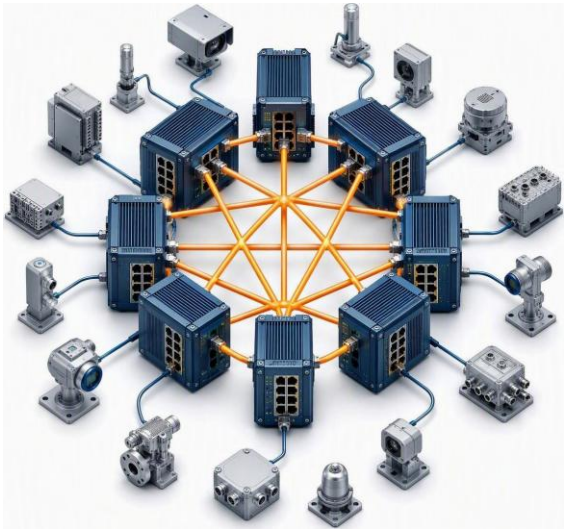
Identifies which sub-graphs will survive multiple, simultaneous node failures.

INDUSTRIAL RELATION

Explains the mathematical resilience of ring topologies, redundant controller pairs, and HA backbones.

AI POTENTIAL

Agents can simulate sequential hardware failures to identify the true k-core resilience of a plant.



Heuristic 8: Network Motifs

WHAT IT EXPLAINS

Complex architectures are built from recurring, predictable micro-structural patterns.

NETWORK VALUE

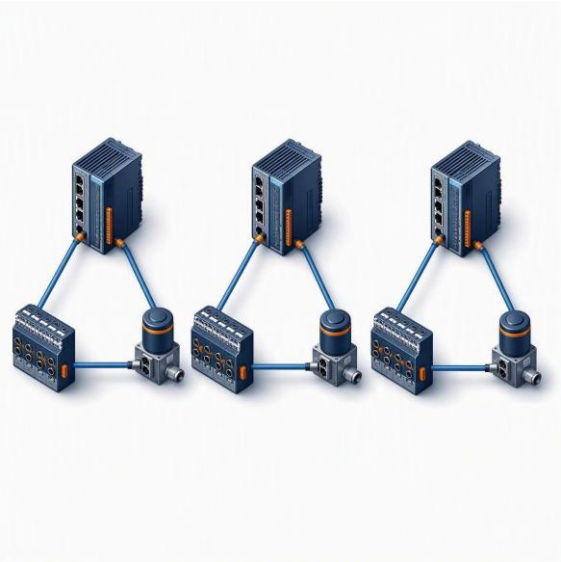
Allows massive systems to be analyzed as combinations of simple, understood building blocks.

INDUSTRIAL RELATION

Explains the structural repetition of standardized machine-builder skids and I/O drops.

AI POTENTIAL

Agents can scan large topologies to verify that all deployed motifs match approved safety templates.



Heuristic 9: Interdependent Failures

WHAT IT EXPLAINS

One network’s failure propagates nonlinearly into another coupled network.

NETWORK VALUE

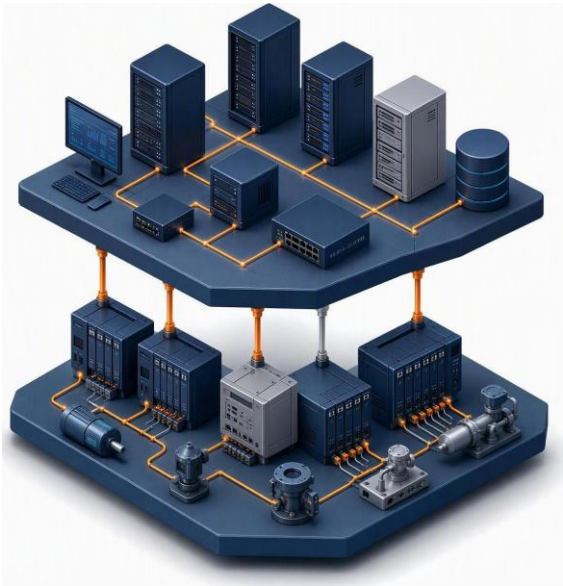
Highlights extreme risks in converged infrastructure that look perfectly safe in isolation.

INDUSTRIAL RELATION

Explains OT control networks dropping because they rely on shared IT DNS or virtualization clusters.

AI POTENTIAL

Agents can map hidden cross-domain dependencies before a single IT failure drops the OT plant.



Heuristic 10: Degree Assortativity

WHAT IT EXPLAINS

Formalizes whether hubs connect primarily to other hubs or strictly to peripheral nodes.

NETWORK VALUE

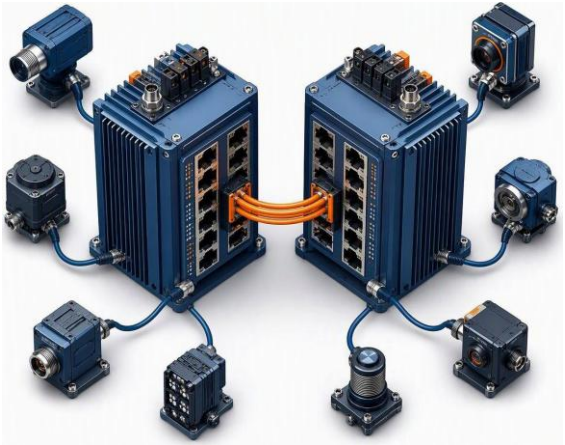
Determines whether the network core is highly integrated or strictly hierarchical.

INDUSTRIAL RELATION

Distinguishes between flat, meshed IT backbones and strict Purdue-model tiering.

AI POTENTIAL

Agents can automatically flag when unauthorized peer-to-peer hub links break the intended security hierarchy.



How the heuristics inform architecture review

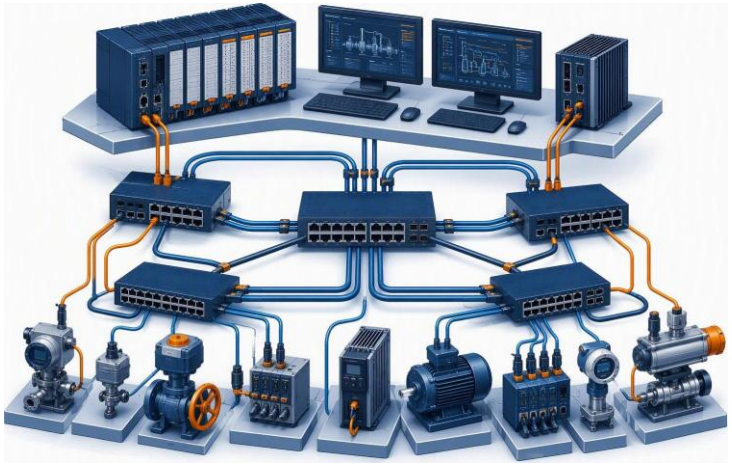
Ten heuristics provide structural clues. Six dimensions turn them into engineering questions.

REVIEW DIMENSION	HEURISTIC CONNECTION	ENGINEERING QUESTION
Topology (21)	Modularity, k-core decomposition, network motifs	How is the network structured?
Interaction density (22)	Triadic closure	Where does repeated activity cluster?
Path significance (23)	Betweenness centrality, brokerage, k-core decomposition	Which routes carry critical dependencies?
Concentration (24)	Preferential attachment, degree assortativity, information cascades	Where do hubs coordinate or amplify risk?
Function fit (25)	A purpose check across all ten heuristics	Does each exchange serve its intended role?
Boundary quality (26)	Modularity, brokerage, interdependent failures	Are crossings observable and recoverable?

Connections are many-to-many. Function fit adds operational purpose to structural analysis.

Heuristics: slides 10–19 Architecture dimensions: slides 21–26

The arrangement of devices and the links between them.



INDUSTRIAL CONTEXT

A topology map shows controllers, switches and I/O connections. It establishes the structure, but does not explain every operational dependency.

Which dependencies remain invisible on the connection map?

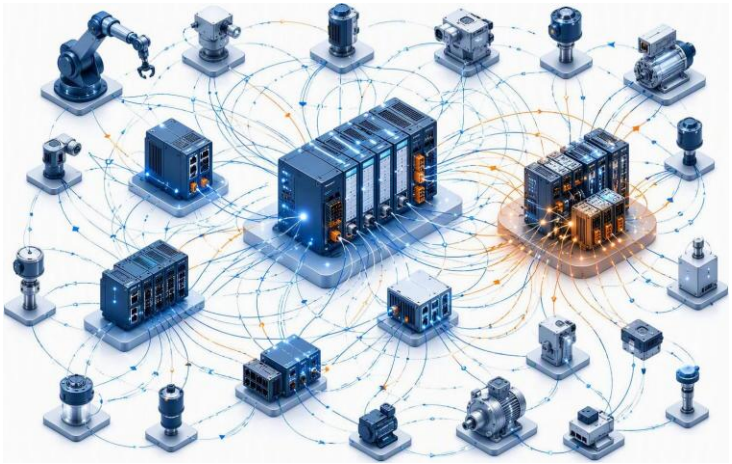
 © 2026 ODVA, Inc.

All rights reserved.

The amount and distribution of communication across the network.

INDUSTRIAL CONTEXT

A controller may exchange frequent local messages yet have limited reach. More traffic alone does not establish wider influence or better visibility.



Where is communication busiest, and what purpose does it serve?

 © 2026 ODVA, Inc.

All rights reserved.

The operational importance of a communication route.

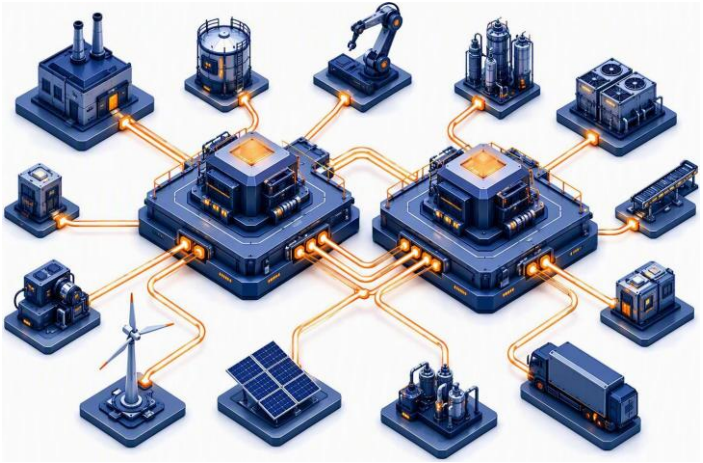


INDUSTRIAL CONTEXT

A route matters when coordination depends on it. Extra paths can support resilience when they have a defined role, or add unnecessary cross-coupling.

What depends on this route, and what happens if it is lost?

The extent to which coordination depends on a few hubs.



INDUSTRIAL CONTEXT

Hubs simplify coordination, but many dependent connections can concentrate fragility. Comparing centralized and bounded dual hubs makes those dependencies easier to assess.

Where would overload or a hub failure affect the most dependents?

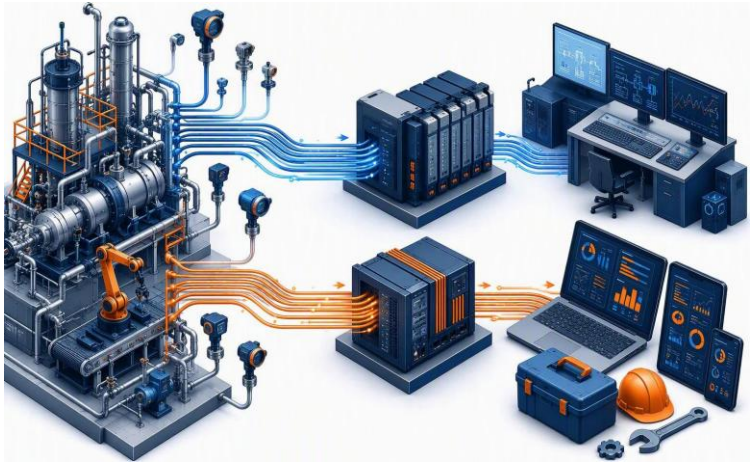
 © 2026 ODVA, Inc.

All rights reserved.

How closely communication behavior matches its operational purpose.

INDUSTRIAL CONTEXT

Control and diagnostics serve different needs. Function-aligned traffic supports each role without indiscriminate high-frequency polling.



Does each traffic pattern support its declared role?

How clearly a boundary exposes and governs cross-zone communication.

INDUSTRIAL CONTEXT

Segmentation needs visible bridge behavior and clear recovery expectations. Hidden dependencies can turn a boundary into a difficult-to-diagnose chokepoint.



Can you see what crosses the boundary and how it recovers?

 © 2026 ODVA, Inc.

All rights reserved.

Heuristic analysis motivates traffic-function declarations

1 MODEL INSIGHT

Structure reveals dependency

Clustering, brokerage and hub concentration show where exchanges matter.

Function fit asks whether those exchanges serve the intended task.

2 INFORMATION GAP

Transport does not declare purpose

A CIP explicit message may support diagnostics, commissioning or configuration.

Its traffic category alone cannot establish the intended function.

3 PROPOSED ENHANCEMENT

Declare the intended function

An optional profile maps supported functions to existing traffic categories.

Read-only disclosure supports architecture review and repeatable commissioning.

The declaration documents intent. It does not infer message semantics or change QoS behavior.

2026 Industry Conference & 24th Annual Meeting
All rights reserved.

Heuristics support engineering decisions today

They describe interaction and dependency, which exist in conventional networks without embedded AI.

HEURISTIC LENS	EVIDENCE AVAILABLE TODAY	ENGINEERING USE
Clustering and modularity	Topology maps and observed exchanges	Check whether cell boundaries match actual communication.
Centrality and brokerage	Approved routes and service dependencies	Identify critical gateways and test loss of a shared path.
Hub growth and cascades	Connection counts, load and fault records	Review capacity, shared dependencies and recovery behavior.
Function fit*	Traffic roles and polling schedules	Check that control, diagnostics and configuration serve distinct needs.

Engineers can apply the framework manually or with offline analysis.
Embedded AI is optional, not a prerequisite for architecture review.

*Function fit adds operational purpose to the structural heuristics.

13.1 Expansion 1: Traffic Function Profile Expansion

Rationale

EtherNet/IP already provides defined traffic treatment categories through the QoS Object, including DSCP values for Class 0/1 priority categories, CIP explicit messaging, and IEEE 1588 traffic.2 The current categories describe traffic transport and priority, but do not provide a standardized way for an application profile to state the intended operational function of a traffic pattern—for example, local cyclic control, supervisory monitoring, commissioning, diagnostics, or time synchronization.

The proposed profile therefore does not attempt to inspect CIP application semantics or assign a new DSCP value to every use case. That would be ambiguous: a CIP explicit message can be used for diagnostics, commissioning, configuration, or other functions. Instead, the profile provides a declarative, profile-level way to document which existing EtherNet/IP traffic categories are intended for defined application functions. This supports architecture review and commissioning repeatability without changing packet formats or mandatory QoS behaviors.1 2



 © 2026 ODVA, Inc.

All rights reserved.

Traffic Function Profile Expansion
Proposed specification locations

Add an informative policy subsection after the Chapter 3 QoS requirements and a normative optional-profile subsection after Volume 2, Chapter 5, Section 5-7: QoS Object.

Proposed location	Proposed title	Function
3-7.x	Traffic Function Policy Guidance	Defines the non-normative relationship between operational function and existing traffic categories.
5-7.x	Traffic Function Profile Declaration	Defines optional read-only declaration and conformance behavior.

2026 Industry Conference & 24th Annual Meeting
All rights reserved.

13.2 Expansion 2: Multicast Governance Expansion

Rationale

Volume 2 already specifies multicast connection handling, recommends unique multicast addresses per active connection, provides multicast-address allocation mechanisms, and defines a multicast TTL configuration whose default value is one. It also cautions users about increasing multicast TTL beyond one.2

The gap is not the absence of multicast mechanics. The gap is the absence of a concise deployment-level declaration that tells an engineer whether an implementation can expose and govern the relevant multicast controls in a routed or segmented deployment. The proposed expansion does not change multicast allocation or make unique address allocation mandatory; it makes the existing configuration state and its deployment implications more explicit.1 2

Recommended Location

Add a new optional conformance profile after Chapter 3, Section 3-3.9: multicast connection rules, with supporting read-only disclosure associated with the TCP/IP Interface Object, Class Code 0xF5.

Proposed location	Proposed title	Function
3-3.9.x	Multicast Governance Profile	Defines the deployment and configuration disclosure requirements.
5-4.x	Multicast Governance Capability Declaration	Defines optional TCP/IP Interface Object disclosure attributes.

2026 Industry Conference & 24th Annual Meeting
All rights reserved.

Multicast Governance Expansion

Proposed Specification Text

3-3.9.x Multicast Governance Profile

This section defines an optional Multicast Governance Profile for an EtherNet/IP device that supports IP multicast for CIP Transport Class 0 or Class 1 connections.

A device that implements the Multicast Governance Profile shall disclose, for each applicable TCP/IP Interface Object instance, the multicast configuration controls supported by that interface.

The profile shall not change the multicast address-selection rules, multicast connection semantics, or consumer packet-screening requirements defined elsewhere in this specification.

A device that implements the profile shall support read access to the TTL Value and Mcast Config attributes for each applicable TCP/IP Interface Object instance.

If the device supports setting either the TTL Value or Mcast Config attribute, it shall document whether an existing multicast connection is affected immediately, affected after reconnection, or requires device restart or other configuration application behavior.

A device shall not automatically increase the multicast TTL Value in response to establishing a connection, receiving a message, detecting a router, or detecting a multicast listener.

When the configured multicast TTL Value is greater than one, the device shall make a read-only indication available through the profile-defined disclosure mechanism. The indication shall not imply that cross-subnet multicast is appropriate, authorized, or supported by the surrounding infrastructure.

The profile shall not require discovery of multicast routers, IGMP queriers, multicast listeners, remote subnets, switch configuration, or end-to-end multicast delivery state.

2026 Industry Conference & 24th Annual Meeting
All rights reserved.

Multicast Governance Expansion

Capability declaration and scope

5-4.x Multicast Governance Capability Declaration

A TCP/IP Interface Object instance that implements the Multicast Governance Profile shall make the following read-only information available:

Attribute	Required behavior
Multicast Governance Profile Revision	Identifies the profile revision supported by the interface.
TTL Configuration Support	Indicates whether the TTL Value attribute is supported and whether it is settable.
Multicast Allocation Support	Indicates whether the Mcast Config attribute is supported and whether the implementation supports default allocation, configured allocation, or both.
Configured Multicast Scope Indication	Indicates whether the configured TTL Value is one, greater than one, or not supported. This indication shall report configuration state only.
Configuration Application Behavior	Indicates whether a change to multicast configuration applies immediately, applies to subsequently established connections, requires reconnection, or requires restart.

Multicast Governance Profile Conformance Statement

A device claiming conformance to the Multicast Governance Profile shall identify the supported profile revision and the TCP/IP Interface Object instances to which the profile applies.

Scope Boundary

This expansion exposes configuration capability and state, not end-to-end multicast correctness. It does not mandate IGMP snooping, multicast routing, unique multicast addresses, or a specific switch configuration. Those are deployment and infrastructure decisions outside a single EtherNet/IP endpoint’s complete visibility.2

All rights reserved.

13.3 Expansion 3: Bridge and Boundary Diagnostics

Rationale and proposed location

Author proposal in Section 13.3

A segmented network can remain protocol-conformant while a gateway or forwarding device becomes an unobserved dependency.

The proposed profile exposes local forwarding behavior so engineers can review and diagnose boundary crossings.

Recommended location in the paper

Proposed location	Purpose
Chapter 10, Sections 10-2–10-2.7	Optional EtherNet/IP-specific CIP bridge and boundary diagnostics.
Appendix G, informative mapping	Optional SNMP mapping for devices that also implement an SNMP Agent.

2026 Industry Conference & 24th Annual Meeting
All rights reserved.

Bridge and Boundary Diagnostics

Proposed disclosure and diagnostic attributes

Read-only local evidence, summarized from Sections 10-2.2–10-2.3

Declare bridge-instance count and identifiers, associated local interfaces, and applicable encapsulation transport modes.

Attribute	Meaning and reporting boundary
Forwarded CIP communication count	Increasing count since discontinuity. State whether units are messages, packets or connection events.
Forwarding discard count	Locally detected discards attributable to that bridge instance.
Forwarding error count	Locally detected errors. Do not infer remote-path faults without local evidence.
Counter discontinuity indicator	Changes when counters reset, restart or lose continuity.
Administrative state	Enabled, disabled or not determinable by the device.

2026 Industry Conference & 24th Annual Meeting
All rights reserved.

Bridge and Boundary Diagnostics

Access constraints, conformance and scope

Summarized from Sections 10-2.4–10-2.7

Access and conformance

Read-only attributes with documented update behavior.

No required cyclic production, unsolicited notification or change to real-time transport.

Claim the supported profile revision, bridge-instance count and supported attributes.

Scope boundary

No required end-to-end latency, remote topology, upstream utilization or inferred health score.

No claim of firewall capability, security enforcement or complete-path validation.

Optional SNMP mapping must preserve CIP-visible semantics.

 © 2026 ODVA, Inc.

All rights reserved.

Expansion 4: Concentration and Chokepoint Health

Access constraints, scope and conformance

Proposed 10-2 Bridge and Boundary Diagnostics Profile

Access and management

Read-only attributes with documented update behavior. Sampled or aggregated data must not appear instantaneous.

No required cyclic production, unsolicited notification or real-time transport change.

Optional SNMP MIB mapping preserves CIP-visible semantics.

Limits of the claim

No required end-to-end latency, upstream utilization, remote topology or peer identity, zone identity, route completeness or inferred health score.

No claim of firewall functionality, security-policy enforcement, zone separation, cybersecurity conformance or end-to-end path validation.

Conformance declaration

Identify the supported profile revision, bridge-instance count, and supported diagnostic attributes for each instance.

2026 Industry Conference & 24th Annual Meeting
All rights reserved.

Expansion 5: Segmented Deployment Profile

Rationale, proposed location and scope

Proposed 10-2 Bridge and Boundary Diagnostics Profile

Why the profile matters

A protocol-conformant segmented network can still depend on an unobserved gateway or forwarding device.

Local boundary evidence helps engineers review and diagnose that dependency.

Where it applies

Optional for devices performing EtherNet/IP-specific CIP bridging or routing across two or more local interfaces.

A bridge instance is a local forwarding function, not necessarily a zone, firewall or complete path.

Recommended location

Chapter 10: add 10-2 through 10-2.7 after the introduction.

Appendix G: optional informative SNMP mapping for devices with an SNMP Agent.

2026 Industry Conference & 24th Annual Meeting
All rights reserved.

Expansion 5: Segmented Deployment Profile

Profile disclosure and diagnostic attributes

Proposed 10-2 Bridge and Boundary Diagnostics Profile

Disclose bridge count, unique local instance IDs, associated interface IDs and applicable encapsulation transport modes through explicit-message diagnostics or a read-only object.

Read-only attribute	Required behavior
Forwarded CIP communication count	Monotonically increases since discontinuity. State the unit: message, packet or connection event.
Forwarding discard count	Monotonically counts locally detected discards since discontinuity.
Forwarding error count	Monotonically counts locally detected errors. Report remote faults only when locally determinable.
Counter discontinuity indicator	Changes when counters reset, restart or lose continuity.
Administrative state	Administratively enabled, disabled or not determinable by the device.

Unsupported attributes use the applicable standard CIP service or attribute-access behavior.

All rights reserved.

Expansion 5: Segmented Deployment Profile

Access constraints, scope and conformance

Proposed 10-2 Bridge and Boundary Diagnostics Profile

Access and management

Read-only attributes with documented update behavior. Sampled or aggregated data must not appear instantaneous.

No required cyclic production, unsolicited notification or real-time transport change.

Optional SNMP MIB mapping preserves CIP-visible semantics.

Limits of the claim

No required end-to-end latency, upstream utilization, remote topology or peer identity, zone identity, route completeness or inferred health score.

No claim of firewall functionality, security-policy enforcement, zone separation, cybersecurity conformance or end-to-end path validation.

Conformance declaration

Identify the supported profile revision, bridge-instance count, and supported diagnostic attributes for each instance.

 © 2026 ODVA, Inc.

All rights reserved.

What This Means for EtherNet/IP Architecture Review

CHECK 1

Can you see traffic roles?

CHECK 2

Can you see chokepoints?

CHECK 3

Can you see boundary crossings?

CHECK 4

Can you repeat the deployment safely?

If a behavior shapes quality, it should be visible enough to review.

 © 2026 ODVA, Inc.

All rights reserved.



Necessary, but not enough.

Discipline beats density.

Specify the behavior.

Better network thinking leads to better architecture and better specification decisions.

The Central Proposition

Similar topologies can produce very different outcomes.

ONE OUTCOME

Resilient. Diagnosable. Scalable.

ANOTHER OUTCOME

Fragile. Opaque. Brittle.

Visible structure alone does not predict system quality.

 © 2026 ODVA, Inc.

All rights reserved.

Literature Support

QUALIFICATION 1

Frequency is not reach.

QUALIFICATION 2

More vectors are not automatically better.

QUALIFICATION 3

Hub importance is conditional.

Simple network rules help, but only when they are qualified by context.

 © 2026 ODVA, Inc.

All rights reserved.

Engineering Consequence of Main Point 1

An architecture review that stops at topology and protocol is incomplete.

Where does coordination concentrate?

Which paths matter most?

Which boundaries conceal fragility?

If you cannot answer these questions, you do not yet understand the architecture.

All rights reserved.

Main Point 2: Discipline Beats Density

The best-performing networks are the most disciplined.

More is not the same as better.

Discipline beats density.

All rights reserved.

Old View vs. New View on Connectivity

OLD VIEW

More traffic = more visibility.

More paths = more resilience.

More hubs = better coordination.

NEW VIEW

Traffic must fit function.

Paths must be purposeful.

Hubs must stay bounded.

Added communication helps only when it is disciplined.

Experimental Method

EtherNet/IP scenarios	Monte Carlo comparison	Weighted factors	1,000 trials

These experiments compare architecture patterns, not protocol conformance.

Cross-Experiment Summary

01 **Broader-reach controller**

02 **Purposeful path diversity**

03 **Function-aligned patterning**

04 **Bounded dual hubs**

05 **Disciplined bridge governance**

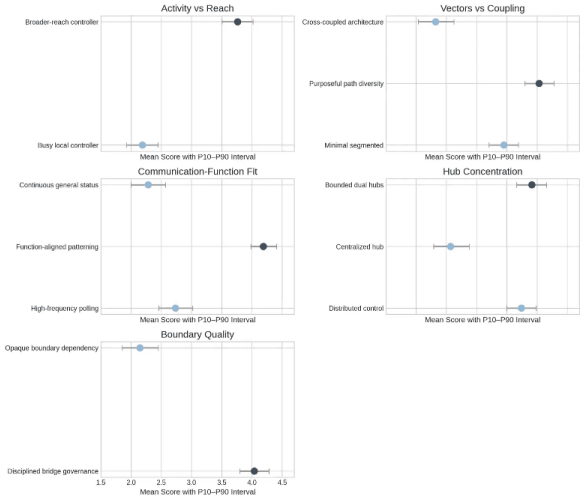
Across five experiments, the governed design wins every time.

All rights reserved.

Winning Variants by Mean Score

The winners are not the busiest. They are the most governed.

Figure 3. Score Distributions by Experiment Variant



Across the experiments, disciplined choices keep finishing on top.

All rights reserved.

Experiment 1: Activity Does Not Equal Reach

WINNING PATTERN

Broader-reach controller

3.762

100% wins

LOSING PATTERN

Busy local controller

2.188

0% wins

High activity is not the same as high reach.

 © 2026 ODVA, Inc.

All rights reserved.

Experiment 2: More Vectors Can Help or Harm

WINNING PATTERN

Purposeful path diversity

Extra paths with a job

LOSING PATTERN

Cross-coupled architecture

Extra paths without discipline

Extra paths help only when they are purposeful.

 © 2026 ODVA, Inc.

All rights reserved.

Experiment 3: Communication-Function Fit

WINNING PATTERN

Function-aligned patterning

Traffic matches purpose

LOSING PATTERN

General high-frequency polling

Traffic outruns purpose

Traffic should match function, not just volume.

 © 2026 ODVA, Inc.

All rights reserved.

Experiment 4: Hubs Help Until They Concentrate Fragility

WINNING PATTERN

Bounded dual hubs

Coordination without overload

LOSING PATTERN

Centralized hub

Coordination with fragility

Hubs help until they concentrate fragility.

 © 2026 ODVA, Inc.

All rights reserved.

Experiment 5: Boundary Quality Governs Segmentation Quality

WINNING PATTERN

Disciplined bridge governance

Visible, bounded, recoverable

LOSING PATTERN

Opaque boundary dependency

Hidden, fragile, unclear

Segmentation works only when boundaries are visible and governed.

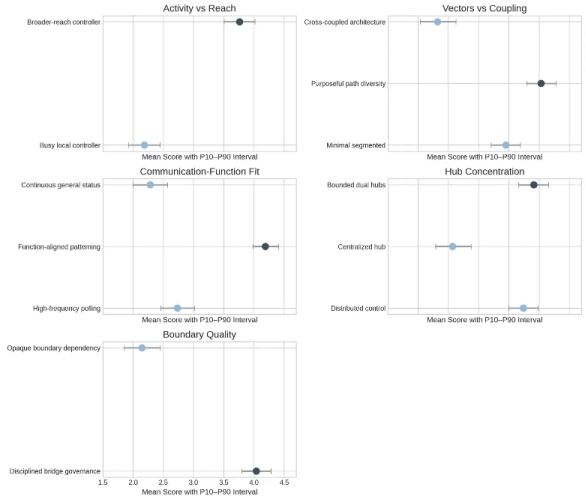
 © 2026 ODVA, Inc.

All rights reserved.

Score Intervals Across Experiment Variants

The stronger variants stay ahead across the modeled range.

Figure 3. Score Distributions by Experiment Variant



The leaders separate clearly from the weaker designs.

Synthesis of Main Point 2

01 **Busyness is not significance.**

02 **Paths must be purposeful.**

03 **Traffic must fit function.**

04 **Concentration must stay bounded.**

05 **Boundaries must be governed.**

The experiments show disciplined architectures outperform dense, busy, and opaque ones.

If architectural behavior matters, the specification should help reveal it.

The paper is not only diagnostic. It is constructive.

All rights reserved.

Evidence for Main Point 3

PROOF 1

The framework points beyond topology.

PROOF 2

The experiments reward disciplined behavior.

PROOF 3

The expansion work becomes standards guidance.

If behavior shapes outcomes, it deserves specification attention.

All rights reserved.

The Five Specification Expansions

01 **Traffic Function Profile**

02 **Multicast Governance**

03 **Bridge and Boundary Diagnostics**

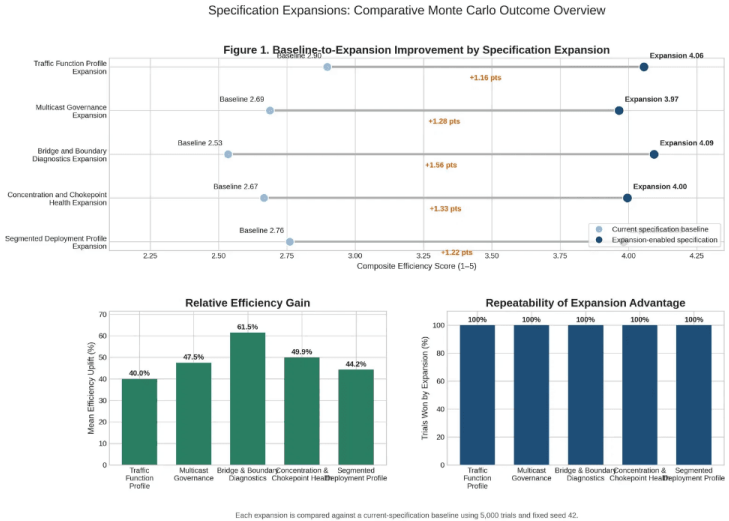
04 **Concentration and Chokepoint Health**

05 **Segmented Deployment Profile**

Five expansions make architectural behavior more visible, governable, and repeatable.

Specification Expansion Overview

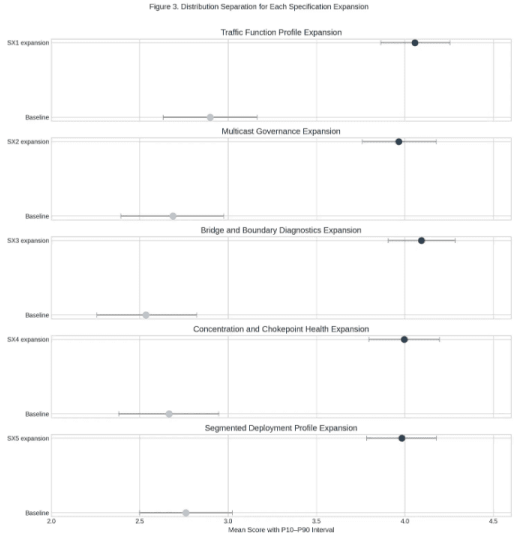
All five expansions beat the baseline.



Modeled architectural behavior can be improved through specification guidance.

Expansion Intervals and Ranked Uplift

Some expansions show bigger and more repeatable gains than others.



Not all wins are equal, but every modeled expansion beats the baseline.

All rights reserved.

SX1: Traffic Function Profile — The Root Problem

THE EVIDENCE

Experiment 3 proved that **function-aligned communication** outperforms indiscriminate traffic growth.

THE ROOT PROBLEM

Control traffic is silently displaced by bursty diagnostics or polling when roles are undeclared.

SX1: Implementation & Mixed Devices

MANUFACTURER IMPLEMENTATION

Expose traffic role in EDS or management interface. No new transport primitives required.

MIXED-DEVICE REALITY

Legacy devices remain "undeclared." The profile protects compliant control traffic from legacy bursts.

SX1: Economic Ramifications

FOR DEVICE MANUFACTURERS

Win IT/OT convergence bids by proving control traffic is immune to IT polling tools.

FOR END USERS

Eliminate downtime caused when aggressive asset-discovery tools silently saturate control bandwidth.

SX2: Multicast Governance — The Root Problem

THE EVIDENCE

Experiment 2 proved that **additional paths** help only when they are deliberately governed.

THE ROOT PROBLEM

Undocumented cross-subnet reach creates hidden coupling, turning local faults into plant-wide storms.



SX2: Implementation & Mixed Devices

MANUFACTURER IMPLEMENTATION

Require explicit TTL configuration and documented multicast allocation in all routed devices.

MIXED-DEVICE REALITY

Legacy devices still flood blindly. Governed routers filter them, protecting the wider plant.

SX2: Economic Ramifications

FOR DEVICE MANUFACTURERS

Differentiate infrastructure products by offering certified, out-of-the-box multicast containment.

FOR END USERS

Avoid massive production losses caused by accidental, multi-cell broadcast storms.

SX3: Boundary Diagnostics — The Root Problem

THE EVIDENCE

Experiment 5 proved that segmentation protects only when bridges are **transparent and governable**.

THE ROOT PROBLEM

When boundaries fail silently, segmentation acts as a hidden chokepoint, not an isolation layer.



SX3: Implementation & Mixed Devices

MANUFACTURER IMPLEMENTATION

Expose boundary state—bridged connections and constrained forwarding—via standard management objects.

MIXED-DEVICE REALITY

Legacy devices remain opaque. Compliant bridges illuminate the boundaries between them.

SX3: Economic Ramifications

FOR DEVICE MANUFACTURERS

Command premium pricing for edge devices that demonstrably reduce plant-wide troubleshooting time.

FOR END USERS

Slash Mean Time To Recovery (MTTR) by instantly localizing cross-zone communication failures.

SX4: Chokepoint Health — The Root Problem

THE EVIDENCE

Experiment 4 proved that concentration helps coordination—until it concentrates **fragility**.

THE ROOT PROBLEM

Undocumented chokepoints silently exhaust their capacity, causing unpredictable, cascading system failures.

SX4: Implementation & Mixed Devices

MANUFACTURER IMPLEMENTATION

Expose connection counts and graceful-degradation state on all coordination hubs.

MIXED-DEVICE REALITY

Dumb switches obscure load. Compliant hubs report exhaustion before failing.

SX4: Economic Ramifications

FOR DEVICE MANUFACTURERS

Sell high-capacity infrastructure by proving it prevents cascading failures during load spikes.

FOR END USERS

Avoid the massive cost of ripping out infrastructure that silently hit an undocumented limit.

SX5: Segmented Profile — The Root Problem

THE EVIDENCE

The framework proves complex architectures need **explicit interoperability rules** to remain resilient.

THE ROOT PROBLEM

When deployment expectations are implicit, segmented architectures drift into fragile, unrepeatable custom builds.

SX5: Implementation & Mixed Devices

MANUFACTURER IMPLEMENTATION

Conform to a system profile defining bridge roles, traffic containment, and expected recovery states.

MIXED-DEVICE REALITY

Legacy devices operate locally. The deployment profile governs the backbone connecting them.

SX5: Economic Ramifications

FOR DEVICE MANUFACTURERS

Shift from selling commodity components to selling certified, highly profitable system-level architectures.

FOR END USERS

Drastically lower integration costs by buying repeatable profiles instead of fragile custom engineering.