COLLABORATIVE SYSTEMS INTEGRATION

WHITE PAPER · PROCESS CONTROL ARCHITECTURE

Open Process Automation for Oil, Gas, and Refining

An open, standards-based alternative to proprietary PLC and DCS control, and how it compares on interoperability, portability, lifecycle cost, and cybersecurity

Prepared by Collaborative Systems Integration (CSI)

For refining and petrochemical leadership, automation and controls engineering, and procurement

Version 1.0 · August 2026

A note on sourcing and certainty

This paper is written to be useful to people who will make or influence a capital decision, so it distinguishes clearly between what is established, what is vendor claim, and what is still emerging. Figures drawn from third-party analyses are attributed to their source in the text and collected in the References section. Quantitative comparisons of Open Process Automation against traditional systems come predominantly from continuous-process industries such as oil, gas, and chemicals, which is the sector this paper addresses, so they apply here more directly than in most other verticals. Even so, each figure reflects the specific study and plant it came from, and this paper flags where a number should not be generalized. Open Process Automation and the O-PAS standard are evolving, and standard versions and certification programs continue to advance beyond the dates cited here; readers making procurement decisions should confirm current standard versions, certified products, and pricing directly with The Open Group and with suppliers.

Contents

1. Executive Summary

Refineries and petrochemical plants run some of the largest and longest-lived control systems in any industry. It is common to find a distributed control system (DCS) specified twenty or thirty years ago, still running a unit around the clock, and now approaching or past the end of its supported life, surrounded by programmable logic controllers (PLCs) on package units and a separate safety instrumented system. Because these platforms are proprietary, the operator's freedom to modernize is limited by a single supplier's roadmap, spare-parts availability, and pricing. Replacing a DCS is expensive, has to be squeezed into a turnaround window, and, under the traditional model, resets the same lock-in for another two or three decades.

Open Process Automation™ (OPA) is a different way to build the control system. Rather than buying a closed platform from one vendor, the operator buys to an open standard, the O-PAS™ Standard, published by The Open Group®'s Open Process Automation Forum. O-PAS defines standard interfaces so that controllers, input and output modules, applications, and software from different suppliers can interoperate on a common connectivity backbone, and so that control applications can be moved from one conforming platform to another. The stated goals of the standard are to stimulate innovation, lower system lifecycle cost, and give end users more freedom to manage obsolescence.

The central argument of this paper is straightforward. The problems that OPA was created to solve, obsolescence of proprietary hardware, vendor lock-in, rising cybersecurity expectations, and the difficulty of adding modern software to a closed system, are precisely the problems that dominate refining and petrochemicals, the sector where OPA already has its deepest field experience. The architecture and the industry's pain points line up unusually well.

What the evidence shows so far

- **Cost.** A cost analysis presented by Collaborative Systems Integration at the 2024 ARC Industry Forum, based on a modeled continuous-process plant with roughly 14,000 I/O, found approximately 52% lower capital cost for system hardware and software using an O-PAS system versus a traditional DCS, narrowing to about 10% total project savings once system-integration cost was included. A separate 25-year cost-of-ownership study calculated by Wood found roughly 47% savings, rising to an estimated 60% to 70% once the cost of downtime for control-system maintenance was included. These figures come from a modeled continuous-process plant, so they apply to refining and petrochemicals more directly than to any other sector, though each operator should still re-derive them on its own I/O count and plant.
- **Interoperability and portability.** O-PAS is built on widely adopted open standards, notably OPC UA for connectivity, IEC 61131 and IEC 61499 for control logic, and the ISA/IEC 62443 series for cybersecurity. This lets an operator mix conforming products from multiple suppliers and avoid re-engineering the whole system when one component reaches end of life.
- **Cybersecurity.** O-PAS mandates conformance to the ISA/IEC 62443 cybersecurity series, and in August 2024 the Open Process Automation Forum named ISASecure as the exclusive verification provider for those requirements. Security is specified into the architecture rather than added afterward.
- **Maturity.** The most advanced public proof point is ExxonMobil's OPA Lighthouse at its Baton Rouge Resins Finishing Plant, which cut over at the end of 2024 and has since run a live hydrocarbon unit, reportedly without major interruption. Refining is the sector with the most field validation of OPA, though the population of at-scale deployments across the industry is still small.

This paper explains what OPA is, characterizes how it differs from PLC and DCS approaches, compares the three on the dimensions that matter to an operator, maps concrete refining and petrochemical use cases, and lays out a pragmatic, low-risk path to evaluate the architecture without betting a unit on it.

Further reading from CSI

This paper is a sector-focused summary. For the underlying architecture in depth, see Trevor Cusworth's book *Open Process Automation: Architecture, Execution & Transformation*. For where the standard, the suppliers, the integrators, and the economics actually stand this year, see CSI's flagship report, *State of Open Process Automation 2026* (a 40-page assessment published May 2026). To model the economics for a specific facility, CSI provides an OPA lifecycle-cost (ROI) calculator at csi-automation.com/opa-roi-calculator, and CSI Academy offers OPA training for engineering and operations staff at csi-automation.com/academy. All are listed in the References.

2. The State of Automation in Oil, Gas, and Refining

To understand why an open architecture is attractive here, it helps to be specific about how refining and petrochemical control is built today and where it strains.

2.1 A layered patchwork, assembled over decades

A typical refinery does not run one control system. It runs several, layered and stitched together over many turnaround and capital cycles. The main process units are controlled by one or more distributed control systems, often from different vendors and different vintages after decades of expansions and acquisitions. Package units, compressors, and skids arrive with their own PLCs. A separate safety instrumented system, built to IEC 61511, protects the hazardous process. Advanced process control and a historian sit on top, integrating data across all of it. Each layer frequently comes from a different supplier and a different era, and the integration between them is bespoke.

This patchwork works, and it has run the process reliably for a long time. Its weakness is not day-to-day function; it is change. Every upgrade, unit revamp, or technology refresh has to navigate a web of proprietary interfaces, usually inside a narrow turnaround window, and the knowledge of how it all fits together often lives in a small number of long-tenured engineers and integrators.

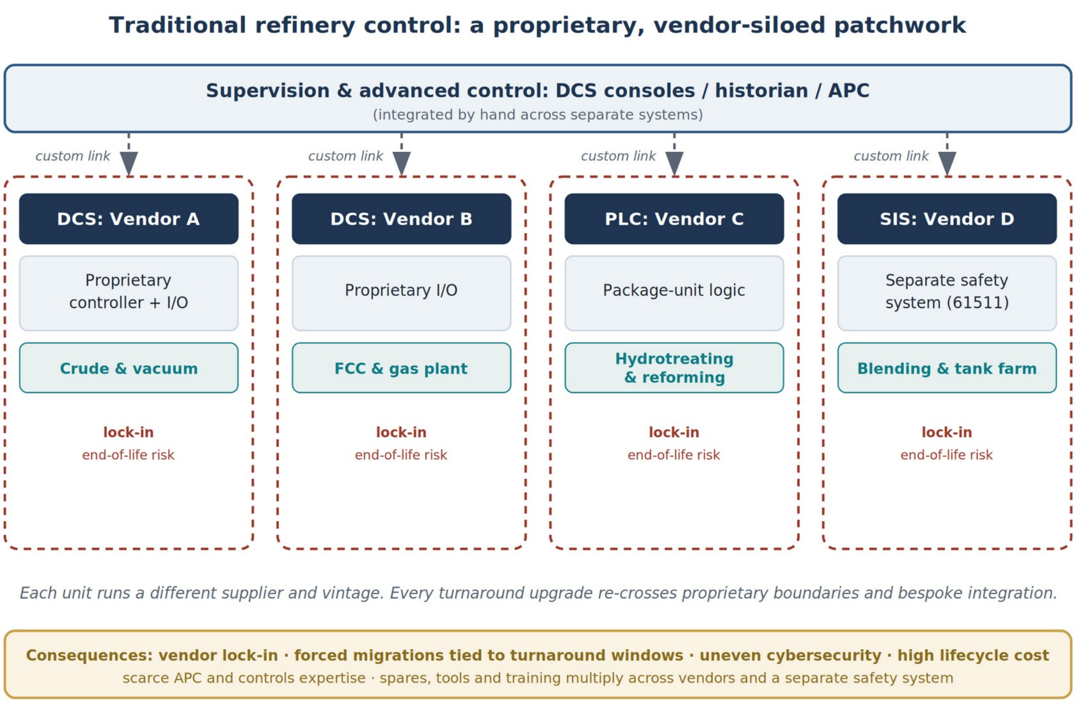

Figure 1. *The traditional refinery control estate is a set of proprietary, vendor-specific silos, one or more DCS platforms, package-unit PLCs, and a separate safety system, stitched together by hand. Each silo carries its own lock-in and end-of-life risk.*

2.2 Aging infrastructure and obsolescence

The installed base is old. Many refinery and petrochemical DCS platforms were installed in the 1990s and 2000s, and a large share are now beyond their originally supported life, kept running through extended-support contracts, harvested spares, and the accumulated knowledge of a shrinking group of engineers. *(The vintage of any given plant's control system varies widely; operators should assess their own installed base and vendor support timelines rather than rely on a sector generalization.)*

Control systems age on a faster cycle than the plant. Processor families go end-of-life, I/O cards become scarce, operating systems fall out of support, and the engineering software needed to modify the system stops running on current computers. When the DCS reaches this point, the operator faces a forced migration, and under a proprietary model the practical choice is usually to buy the successor platform from the same vendor, because that is the path of least disruption during a turnaround. The obsolescence problem is therefore also a lock-in problem.

2.3 Vendor lock-in and proprietary protocols

Traditional control platforms use proprietary hardware and, in many cases, proprietary or semi-proprietary communications between controllers and I/O. That is what ties an operator to one supplier: the controllers, the I/O, the engineering tools, and the spare parts must generally all come from that vendor, and third-party or successor products rarely drop in without re-engineering. When a single supplier's roadmap, lead times, and pricing govern the operator's ability to maintain and expand a production asset that runs around the clock, the operator has surrendered leverage on a decades-long commitment.

2.4 Cybersecurity as a first-order requirement

Refineries, pipelines, and petrochemical plants are designated critical infrastructure, and the operational technology (OT) that runs them is squarely within the threat model, a point underscored by the 2021 Colonial Pipeline ransomware shutdown. Older control systems were designed for isolated networks and often predate modern security expectations, yet they are increasingly connected for remote operations, analytics, and integration with enterprise systems. Retrofitting robust segmentation, authentication, patching, and monitoring onto architectures that were never designed for it is difficult and expensive. Operators need security that is engineered into the control system, not bolted on after commissioning.

2.5 Workforce and knowledge risk

The workforce that built and maintains these systems is retiring, and operators compete for a shrinking pool of controls and advanced-process-control talent. Proprietary platforms compound the problem: each vendor has its own tools, languages, and conventions, so skills are not readily transferable and training is vendor-specific. When the one engineer who understands the legacy configuration leaves, the operator inherits a system it can run but struggles to change safely.

2.6 Safety and advanced control live in separate silos

Two of the most important layers in a refinery, the safety instrumented system and advanced process control, typically sit outside the DCS as separate, proprietary systems with their own engineering environments. The safety system, built to IEC 61511, is deliberately independent for good reasons, but in practice it is also a separate vendor relationship, a separate lifecycle, and a separate integration to maintain. Advanced process control, which delivers much of a unit's margin, is usually a proprietary application layered on top and re-integrated at every migration. An architecture that provides standard interfaces lets these layers connect in a consistent, documented way and lets advanced-control applications move forward rather than being rebuilt each cycle.

2.7 Regulatory pressure is rising

Refining and petrochemicals operate under a dense regulatory framework, and the parts that touch control systems are not relaxing. Process safety is governed by OSHA's Process Safety Management standard (29 CFR 1910.119) and the EPA's Risk Management Program (40 CFR 68), both of which require rigorous management of change and mechanical integrity, disciplines that a well-documented, standards-based control architecture supports. Functional safety follows IEC 61511 (ISA 84). On cybersecurity, the 2021 Colonial Pipeline incident prompted the TSA to issue security directives for pipelines, which the agency has since worked to make permanent through rulemaking, while the Chemical Facility Anti-Terrorism Standards (CFATS) program lapsed in 2023 when its statutory authority expired, leaving a patchwork that voluntary frameworks and ISA/IEC 62443 increasingly fill.

The direction of travel is clear: operational-technology cybersecurity across energy and process industries is moving from voluntary good practice toward enforceable expectation. A control architecture that specifies ISA/IEC 62443 conformance into the system, as O-PAS does, and that can evidence that conformance through third-party certification, is aligned with where the regulatory environment is heading rather than fighting it. *(Regulatory requirements and their status change frequently, and some developments summarized here are recent; operators should confirm current obligations, including the status of TSA directives and CFATS, with the relevant agencies and counsel.)*

2.8 The economics are driven by uptime and turnaround windows

Unlike a public utility, a refinery does not draw on federal infrastructure funds; its economics are driven by throughput and uptime. Unplanned downtime on a major unit is commonly valued in the hundreds of thousands to millions of dollars per day, which makes the reliability and cyber-resilience of the control system a direct margin issue, not an overhead line. At the same time, major control-system work is generally constrained to turnaround windows that come only every few years, so the timing of an obsolescence-driven migration matters enormously. This is where the open architecture's economics are strongest: the cost studies cited in this paper come from exactly this kind of continuous-process plant, and aligning an O-PAS migration with a planned turnaround lets an operator modernize without buying back into another proprietary lifecycle. *(Downtime valuations vary widely by unit, product slate, and market conditions; operators should use their own margin and reliability figures rather than a sector generalization.)*

3. What Is Open Process Automation?

Open Process Automation is an approach to building process control systems from interoperable, standards-based components rather than from a single vendor's closed platform. The technical expression of the approach is the O-PAS Standard.

3.1 Origins and governance

The initiative grew out of work led by ExxonMobil beginning around 2016, driven by frustration with proprietary DCS platforms that were expensive to sustain and slow to accept new technology. ExxonMobil engaged Lockheed Martin as a systems integrator for an early prototype and convened end users and suppliers to define a common standard. That standards work moved to The Open Group, a vendor-neutral standards body, which established the Open Process Automation Forum (OPAF) to develop and maintain the O-PAS Standard. As of 2024, OPAF reported more than 120 member organizations spanning end users, suppliers, system integrators, and academia.

O-PAS (the Open Process Automation Standard) is deliberately described as a "standard of standards." Rather than inventing new technology where good standards already exist, it composes established ones, OPC UA, IEC 61131, IEC 61499, ISA/IEC 62443, and DMTF Redfish among them, into a coherent reference architecture for open, interoperable, secure process control.

3.2 The core architectural ideas

A few concepts carry most of the weight. They are worth understanding because they are exactly what differentiates OPA from a conventional PLC or DCS.

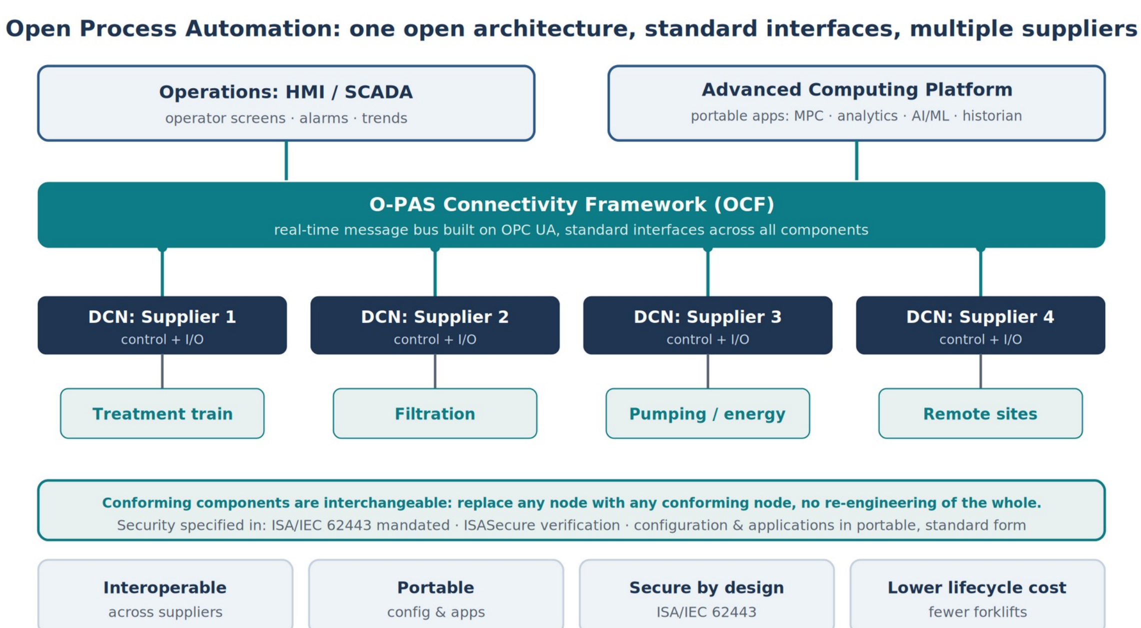

Figure 2. *In an OPA system, conforming components from multiple suppliers connect through the OPC UA-based O-PAS Connectivity Framework. Distributed Control Nodes, applications, and supervision all share standard interfaces, so any conforming component can be replaced without re-engineering the whole.*

Distributed Control Node (DCN)

The DCN is the standard building block of control. It is a compact, comparatively low-cost compute element that performs control, connects to I/O, and speaks the standard interfaces. Instead of a large proprietary controller cabinet, control is distributed across many small conforming nodes, which can, in principle, be sourced from different suppliers because they conform to the same standard.

O-PAS Connectivity Framework (OCF)

The OCF is the standardized connectivity backbone, a real-time message bus that carries data among all the components of the system. It is built on OPC UA, the widely adopted industrial interoperability standard. Because every conforming component connects through the OCF using standard interfaces, a controller from one supplier and an application from another can exchange data without custom integration for each pairing.

Advanced Computing Platform and applications

O-PAS anticipates that meaningful computation, data acquisition, filtering, monitoring, diagnostics, advanced control, and analytics, runs on standard computing platforms and can be deployed as portable applications rather than being locked inside proprietary controllers. This is what makes it practical to add modern software, including model-based control and machine learning, to the control system over its life.

Physical platform and system management

The standard also specifies the physical platform and system-management interfaces, including the use of DMTF Redfish for hardware management, so that conforming devices can be managed in a consistent, vendor-neutral way.

3.3 The three properties that matter: interoperability, portability, and configuration portability

OPA's value is best understood through three related but distinct properties. Procurement and engineering teams should be precise about them, because vendors sometimes use them loosely.

1. **Interoperability.** Components from different suppliers can exchange data and work together through standard interfaces. This is what breaks the requirement that controllers, I/O, and applications all come from one vendor.
2. **Configuration portability.** The configuration of the system, its setup and parameters, can be expressed in a standard form so it is not trapped in one supplier's proprietary engineering tool. O-PAS Version 2 introduced configuration portability, and Version 2.1 extended it.
3. **Application portability.** A control application written to the standard can be moved from one conforming platform to another without being rewritten. This is the most powerful property for long-term obsolescence management, and it is the focus of the forum's work toward Version 3.0.

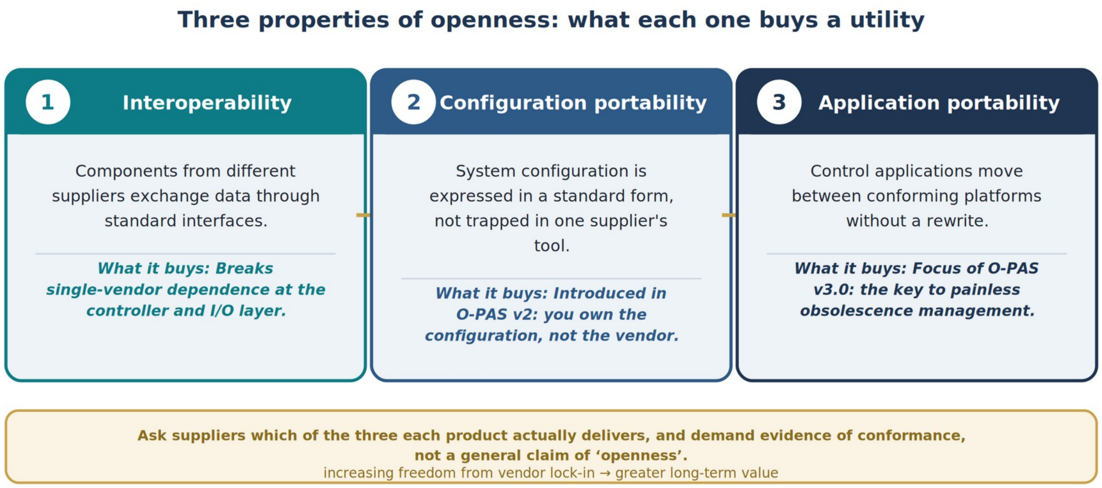

Figure 3. *Interoperability, configuration portability, and application portability are distinct properties. A product can deliver one without the others, so an operator should ask specifically which it provides and require evidence of conformance.*

Why the distinction matters for an operator

Interoperability lets you buy the best component today. Portability lets you replace a component in fifteen years without re-engineering the control logic that runs your plant. A supplier can be interoperable at the connectivity layer while still making your applications hard to move. When evaluating products, ask specifically which of the three properties a product delivers, and demand evidence of conformance rather than a marketing claim.

3.4 Standard structure and versions

The O-PAS Standard is published in parts, each addressing a layer of the architecture. In Version 2.1 the standard comprises the following parts:

Part	Title / scope
Part 1	Technical Architecture Overview (informative)
Part 2	Security
Part 3	Profiles (informative)
Part 4	O-PAS Connectivity Framework (OCF)
Part 5	System Management
Part 6.1–6.6	Information and Exchange Models: overview and interfaces, basic configuration, alarms and events, function blocks, IEC 61499, and IEC 61131
Part 7	Physical Platform

The standard has advanced through successive versions, broadening what "open" delivers at each step:

- **Version 1 (2019)** established interoperability.
- **Version 2 (January 2020)** added configuration portability.
- **Version 2.1 (preliminary standard, 2021)** progressed the information model and extended configuration portability.
- **Version 3.0 (in development)** targets application portability and system orchestration.

Verify current status

Standard versions, part numbering, and certification programs continue to evolve past the dates above and beyond this author's knowledge horizon. Confirm the current published version, conformance program, and list of certified products directly with The Open Group before making procurement commitments.

3.5 Conformance and cybersecurity certification

An open standard is only as good as the ability to verify that a product actually conforms to it. Two mechanisms matter. First, The Open Group operates a conformance program for O-PAS so that products can be certified against the standard rather than merely claiming compatibility. Second, on cybersecurity specifically, O-PAS mandates conformance to the ISA/IEC 62443 series in Part 2, and in August 2024 OPAF selected ISASecure as the exclusive verification provider for those cybersecurity requirements, leveraging ISASecure's network of accredited certification bodies. For an operator, this means security conformance can be evidenced by third-party certification rather than taken on faith.

4. How Traditional Architectures Work, and Where They Strain

OPA is best judged against the systems it would replace or complement. This section characterizes the two dominant traditional approaches fairly, including their genuine strengths, before the structured comparison that follows.

4.1 The Distributed Control System (DCS)

A DCS is an integrated, vendor-supplied platform designed to control a continuous process as a coordinated whole. It bundles controllers, I/O, engineering tools, operator interface, alarming, and historian into one tightly engineered product line. In refining and petrochemicals, the DCS is the backbone of process control, coordinating hundreds or thousands of loops per unit and operated from a central control room.

The strengths are real. A DCS offers a mature, coherent operator environment, strong alarm and batch handling, high reliability, and a single vendor accountable for the whole system. For a large, continuous, safety-relevant process, that integration is valuable. The cost of that integration is closure: the pieces are proprietary and are designed to work together and, by extension, not to be mixed with anyone else's. Lifecycle costs accumulate through the vendor's support contracts, migration cycles, and the practical impossibility of competitive sourcing for controllers and I/O.

4.2 Programmable Logic Controllers (PLCs) and SCADA

Alongside the DCS, refineries use PLCs extensively on package units, compressors, and skids, often paired with SCADA or tied back into the DCS. PLCs are rugged, fast, widely understood, and comparatively inexpensive, and there is a deep labor pool of engineers and integrators who work with the major brands. They are excellent at what they do, but they add another set of proprietary controllers, tools, and interfaces to the estate.

This approach is flexible and cost-effective, but its limitations show up at the system level. The PLC brand is still proprietary at the controller and I/O layer, so lock-in persists even if it feels lighter than a DCS. Integration between PLCs, SCADA, the DCS, and any advanced applications is custom work that must be re-created and re-validated at each upgrade. Cybersecurity is uneven, because it depends on how each layer and each integration was implemented. And portability of the control logic is essentially absent: logic written for one brand does not move to another without a rewrite.

The common thread

Both traditional approaches are proprietary at the layer that matters most for long-term freedom: the controller and I/O, and the engineering tools that configure them. That is the specific point of closure OPA is designed to open. The question is not whether DCS and PLC and SCADA systems work, they plainly do, but whether the operator should keep accepting single-vendor dependence on a production asset with a multi-decade life.

5. OPA versus PLC versus DCS: A Structured Comparison

The table below summarizes the comparison across the dimensions that most affect a refining operator over a system's life. The discussion after it adds nuance, because a summary table necessarily simplifies.

Dimension	Traditional DCS	PLC + SCADA	Open Process Automation
Sourcing model	Single vendor, fully integrated platform	Proprietary PLC brand plus separate SCADA; some multi-vendor mixing	Multi-vendor by design; buy conforming components to one open standard
Interoperability	Within the vendor's ecosystem; limited outside it	Via protocols and custom integration; brand-locked at controller and I/O	Standard interfaces (OPC UA-based OCF) across suppliers
Application portability	Very low; logic tied to platform	Very low; logic tied to PLC brand	A core goal of the standard (advancing toward v3.0)
Obsolescence management	Vendor-driven migration cycles	Component swaps, but brand-locked	Replace conforming parts without re-engineering the whole
Cybersecurity	Vendor-dependent; often retrofit	Uneven; implementation-dependent	ISA/IEC 62443 mandated; ISASecure verification
Advanced apps (MPC, analytics, AI/ML)	Add-on modules, often proprietary	Custom integration required	Portable apps on standard compute platforms
Capital cost profile	Highest for integrated platform	Lower entry cost	Lower hardware/software cost; integration cost still developing
Maturity in oil, gas & refining	High; the sector backbone	High; on package units	Field-validated (ExxonMobil); still early industry-wide

5.1 Interoperability

The decisive difference is at the controller and I/O layer. In both traditional models, that layer is proprietary, which is what sustains lock-in. OPA standardizes the interfaces there, and connects everything through the OPC UA-based OCF, so conforming products from different suppliers interoperate without one-off integration. For an operator, the practical payoff is competitive sourcing and the ability to introduce a better component without replacing the surrounding system.

5.2 Portability and obsolescence

This is where OPA's long-term value concentrates, and where it most directly answers the refining sector's central pain. Under the traditional model, obsolescence forces a migration that is effectively a re-implementation, and it resets vendor lock-in for the next cycle. Under OPA, configuration and, increasingly, applications are expressed in standard forms, so a node that reaches end of life can be replaced by any conforming node, and the control logic moves with far less rework. Over a 25-year asset life, this is the difference between one architecture maintained through incremental component refreshes and several disruptive forklift migrations.

5.3 Cybersecurity

Traditional systems vary widely in security posture because it depends on when and how they were built and integrated. OPA specifies security into the architecture by mandating ISA/IEC 62443 conformance and providing third-party verification through ISASecure. This does not make an OPA system automatically secure, security still depends on correct deployment and operations, but it raises the floor and makes conformance verifiable, which matters for a critical-infrastructure operator answerable to regulators.

5.4 Scalability across units and the enterprise

Because control is distributed across small conforming nodes rather than concentrated in large proprietary controllers, OPA scales granularly. An operator can standardize on the same interfaces from a major process unit down to a single package skid, and across multiple plants in a refining network, while still choosing fit-for-purpose hardware at each point. A single standard across many units and sites reduces spares, training, and integration overhead and makes fleet-wide advanced control and analytics far easier to deploy.

5.5 Cost

The most cited cost evidence comes from a Coalition for Open Process Automation analysis presented by Don Bartusiak, president of Collaborative Systems Integration, at the 2024 ARC Industry Forum. Modeling a continuous-process plant with roughly 14,000 I/O against traditional DCS installations, the analysis found approximately **52% lower capital cost for system hardware and software** with an O-PAS system, narrowing to about **10% total project savings** once system-integration cost was included. On a 25-year cost-of-ownership basis, Wood calculated roughly **47% savings**, and when the cost of plant downtime for control-system maintenance was included, customer-calculated savings reached an estimated **60% to 70%**. Analysts expect the integration-cost gap to shrink as application reuse and portability mature.

Read these numbers carefully

These figures come from continuous-process industries (oil, gas, chemicals), which is the sector this paper addresses, so they apply here more directly than in most verticals; still, they reflect a specific modeled plant and specific assumptions. They are a strong indicator that open architecture lowers hardware and lifecycle cost, but they are not a substitute for a plant-specific model. Any business case should be built on the operator's own I/O count and unit configuration, and should treat the single-digit near-term project savings, not the headline capital figure, as the conservative planning number until integration costs mature.

6. Applying OPA to Oil, Gas, and Refining

The abstract advantages become concrete when mapped to the situations refiners actually face. The following use cases are where the architecture's fit is strongest. None of them requires the operator to convert everything at once.

6.1 Turnaround-aligned DCS modernization

A unit whose DCS is at end of support faces a forced migration, and that migration has to happen during a turnaround. This is the natural entry point for OPA, because the operator is already spending the capital and accepting the outage. Specifying the replacement to O-PAS conformance converts a like-for-like forklift into a one-time move to an architecture that will not force the same lock-in again. The operator spends similar money but buys future optionality instead of another proprietary cycle.

6.2 Standardizing across units, packages, and plants

Process units, package skids, and multiple plants accumulate a mix of DCS and PLC platforms from many projects and eras. Adopting a common set of standard interfaces across new and revamped units lets the operator reduce the number of distinct platforms it must stock spares for, train staff on, and integrate. Distributed control nodes suit both large units and small package equipment, and a consistent connectivity model across the site simplifies the integration that today is re-engineered unit by unit.

6.3 Adding advanced control and optimization

Refining margin depends heavily on advanced process control and real-time optimization, on crude units, FCC, reformers, and blending, where model predictive control and analytics capture yield and energy savings measured against every barrel. In a closed system, each such application is a custom, proprietary integration that is rebuilt at every DCS migration. OPA's model of portable applications running on standard compute platforms makes it materially easier to deploy and, crucially, to carry advanced process control and machine-learning applications forward as the control hardware is refreshed rather than rebuilding them each time.

6.4 Enterprise-wide architecture across a refining network

An operator running several refineries and petrochemical sites benefits from a single architectural standard across all of them: common interfaces, common security requirements, transferable staff skills, and consolidated spares. OPA provides that standardization at the interface level without forcing every site onto identical hardware, which matters when sites differ widely in configuration and vintage.

A realistic note on adoption

Refining has the most OPA field experience of any sector: ExxonMobil's Lighthouse cut over at Baton Rouge at the end of 2024 and has run a live hydrocarbon unit since. Even so, the number of publicly documented, at-scale deployments across the industry is still small, so an operator adopting OPA now remains an early adopter. That carries real advantages, influence over the ecosystem, competitive sourcing, and a head start on obsolescence, but it also means a limited set of directly comparable references, which argues for the phased, pilot-first approach described in the next section.

7. A Practical Migration Path

Operators cannot and should not replace working control systems wholesale, and OPA does not require them to. The sound approach is incremental, evidence-driven, and designed so that each step delivers value on its own while building toward the target architecture.

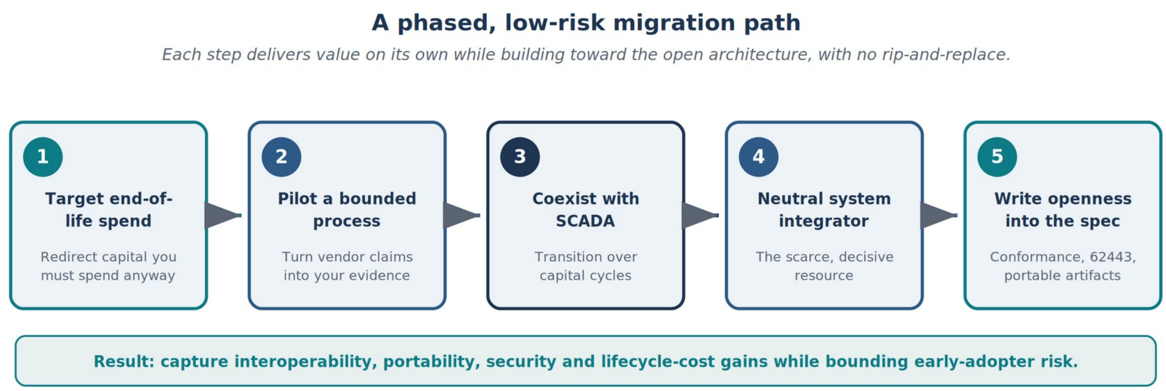

Figure 4. *A phased path lets an operator adopt OPA where obsolescence is already forcing spend, prove it on a bounded pilot, and expand through coexistence, rather than a single high-risk replacement.*

7.1 Start where obsolescence is already forcing spend

Identify assets already scheduled for control-system replacement, a unit whose DCS is at end of life and slated for the next turnaround, or a package system due for refresh. Directing capital that would be spent anyway toward O-PAS-conforming equipment is the lowest-risk way to begin, because the alternative is not "do nothing," it is "buy proprietary again."

7.2 Pilot on a bounded, non-critical process

Choose a contained plant utility system or a non-critical package unit where failure modes are well understood and the consequences of problems are manageable. Use the pilot to validate conformance claims from suppliers, exercise the OPC UA-based connectivity in the operator's real network, test the security posture, and build internal familiarity. The pilot's purpose is to convert vendor claims into the operator's own evidence.

7.3 Coexist, do not rip and replace

OPA components can interoperate with existing SCADA and, through standard connectivity, with parts of the legacy system, so the transition can be gradual. New and refreshed assets move to the open architecture while the rest of the plant continues to run, and the two coexist through the SCADA layer during a transition that can span multiple turnaround cycles.

7.4 Use an experienced, vendor-neutral system integrator

The value of an open architecture is realized in integration, and today integration expertise is the scarcer resource, which is exactly why near-term project savings are smaller than the headline hardware savings. A system integrator with genuine OPA experience and a vendor-neutral stance, rather than an integrator effectively tied to one platform, is central to a good outcome. This is the specific gap Collaborative Systems Integration exists to fill. Operators that want to build capability in-house can also train engineering and operations staff directly through CSI Academy (csi-automation.com/academy), which shortens the learning curve and reduces dependence on any single integrator over the asset's life.

7.5 Write openness into the specification

The architecture only stays open if procurement keeps it open. Specifications and contracts should require demonstrated O-PAS conformance and ISA/IEC 62443 verification, should call out interoperability, configuration portability, and application portability explicitly rather than accepting a general claim of "openness," and should require that configuration and application artifacts be delivered in the standard, portable forms so the operator, not the supplier, controls them over the asset's life.

8. Cost and Value Over the Asset Life

Refiners live and die by margin, and control-system decisions bind a unit for two or three decades. That makes lifecycle cost, not just installed cost, the right frame, and it is the frame in which OPA's argument is strongest.

8.1 Capital versus lifecycle

The evidence comes from exactly this kind of continuous-process plant, and separates two effects. The capital-cost advantage of open hardware and software is large in the modeled cases, on the order of 52% for system hardware and software in the CSI-presented analysis. The near-term total-project advantage is much smaller, roughly 10%, because system-integration cost currently offsets much of the hardware saving. The lifecycle advantage is where the case compounds: a 25-year ownership analysis by Wood found roughly 47% savings, and 60% to 70% when the cost of downtime for control-system maintenance was included, a figure that resonates in a refinery where downtime is measured against daily margin.

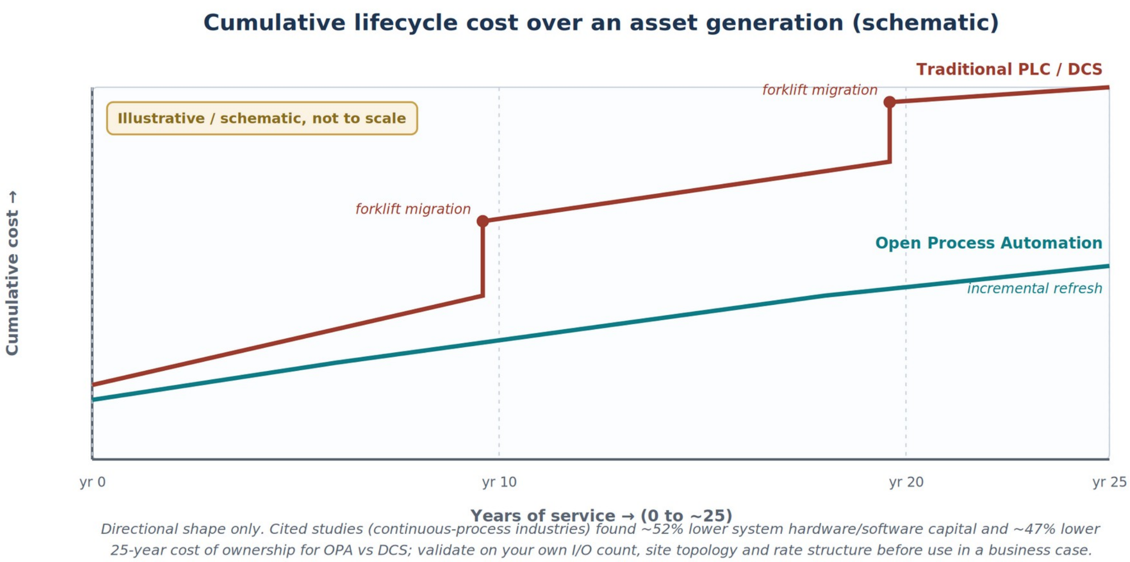

Figure 5. *Schematic of cumulative lifecycle cost. Traditional systems step up at each forced forklift migration; an open architecture is refreshed incrementally. Shape is illustrative only; the cited savings come from continuous-process studies and should be re-derived on an operator's own numbers.*

CSI's flagship report, *State of Open Process Automation 2026*, frames a 60% to 70% lifecycle-cost reduction over 25 years as the headline economic case for open architecture, alongside an assessment of where the standard, suppliers, integrators, and project-execution discipline stand this year. As an assessment authored from inside the standard by former Open Process Automation Forum leadership, it is a well-informed industry view rather than a fully independent audit, and its economics come from the same continuous-process context as this sector. It is a useful next read for an operator building its own business case.

8.2 The value that does not show up as a line item

Several of OPA's benefits are real but harder to price, and an operator's business case should name them even where it cannot precisely quantify them: avoided cost and disruption of future forklift migrations; competitive sourcing leverage on controllers, I/O, and applications instead of sole-source dependence; verifiable cybersecurity conformance in a regulated critical-infrastructure setting; the ability to add and carry forward margin-capturing advanced process control without a proprietary integration each time; and reduced spares and training overhead from standardizing across units and sites.

To turn these effects into facility-specific numbers, CSI publishes an OPA lifecycle-cost (ROI) calculator (csi-automation.com/opa-roi-calculator) that lets an operator model hardware, integration, and 25-year ownership cost against its own I/O count and unit configuration, which is the right way to convert the directional figures above into a defensible business case.

> **The conservative planning posture**
>
> Build the near-term business case on the modest single-digit project savings, not the headline capital figure, and treat obsolescence avoidance and sourcing leverage as the strategic returns that accrue over the asset's life. If integration costs fall as the ecosystem matures, as analysts expect, the near-term case improves; if they do not, the operator has still bought out of the next forced, locked-in migration. Every figure in this section originates in continuous-process studies and should be re-derived on the operator's own numbers.

9. Risks, Limitations, and Honest Caveats

A credible case names its own weaknesses. The following are the real limitations a refining operator should weigh, stated plainly.

- **Industry-wide maturity is still early.** Refining has the strongest field references of any sector, but the total population of at-scale deployments remains small, so an operator adopting now is still an early adopter with a limited set of directly comparable references.
- **Near-term integration cost.** System-integration cost currently offsets much of the hardware saving, which is why near-term project savings are single-digit rather than the headline capital figure. This should improve with ecosystem maturity, but that is an expectation, not a guarantee.
- **The skills to do it well are scarce.** Realizing an open architecture depends on integration expertise that is still concentrated in a small number of practitioners. Choosing the integrator carefully is not optional.
- **The standard is still evolving.** Key properties, most notably full application portability, are maturing through successive versions. Operators should track the current version and certified-product list rather than assume a fixed state.
- **Openness must be actively maintained.** An open standard does not by itself prevent lock-in; an operator that does not write conformance and portability into its specifications and contracts can end up dependent on a single supplier's implementation despite the open label.
- **Procurement models lag.** Turnaround-driven capital planning and existing frame agreements are built around traditional single-vendor projects. Multi-vendor, standards-based sourcing may require adapting specification, evaluation, and contracting practices.

None of these is a reason not to evaluate OPA. They are reasons to evaluate it the way section 7 describes: incrementally, with pilots, with conformance written into contracts, and with an experienced vendor-neutral integrator, so the operator captures the upside while bounding the risk.

10. Recommendations

1. **Treat the next forced control-system replacement as a decision point, not a formality.** When a platform reaches end of life, evaluate an O-PAS-conforming replacement alongside the proprietary successor, and compare them on lifecycle cost and obsolescence exposure, not just installed price.
2. **Run a bounded pilot.** Prove conformance, connectivity, security, and integration on a contained, non-critical process before committing to a broader program, and convert supplier claims into your own evidence.
3. **Standardize interfaces across units and sites.** Adopt common O-PAS-based interfaces for new and revamped units and package systems to cut spares, training, and integration overhead over time.
4. **Write openness and security into every specification.** Require demonstrated O-PAS conformance, ISA/IEC 62443 verification, and delivery of configuration and application artifacts in portable, standard forms, and name interoperability, configuration portability, and application portability explicitly.
5. **Engage a vendor-neutral integrator early.** Integration expertise is the scarce resource and the largest single determinant of outcome; involve it before the architecture is fixed.
6. **Build the business case on your own numbers.** Re-derive cost figures from your I/O counts, unit configuration, and downtime valuations, use the conservative near-term project savings for planning, and carry obsolescence avoidance and sourcing leverage as strategic returns.

11. Conclusion

Refineries and petrochemical plants are, more than most industries, hostage to the longevity and closure of their control systems. They run aging, proprietary, layered systems on critical, high-value production assets, they are pushed to modernize for reliability, margin, and cybersecurity, and under the traditional model every modernization resets the same single-vendor dependence for another two or three decades. Open Process Automation was created, in this very industry, to break exactly this pattern: to make control systems interoperable across suppliers, to make configurations and applications portable, to specify cybersecurity into the architecture, and to lower lifecycle cost by ending the reliance on one vendor's proprietary hardware.

The architecture's fit with refining's problems is unusually clean, and this is the sector where OPA has already been proven in the field. The honest qualifier is maturity: the population of at-scale deployments is still small, near-term integration costs still offset much of the hardware saving, and an operator adopting now does so relatively early. But the strategic direction is clear, and the risk is manageable through a phased, pilot-first, specification-driven approach. For an operator making a decades-long commitment on a production asset, the most consequential choice is not which vendor to buy, but whether to keep buying closed systems at all. Open Process Automation offers, for the first time, a credible alternative.

Appendix A. Frequently Asked Questions

The questions below are the ones refining and petrochemical leaders and engineers most often raise when they first evaluate Open Process Automation. The answers are deliberately direct, including where the honest answer is a qualification.

Is OPA actually proven, or is it still a science project?

It is proven in principle and increasingly in practice. The standard is real and published, conformant products exist, and ExxonMobil's Lighthouse has run a live hydrocarbon unit at its Baton Rouge plant since the end of 2024. What is still thin is a long list of at-scale, publicly documented deployments across the industry. An operator adopting now is an early adopter: that carries genuine advantages, but it is not the same as buying a technology with a thirty-year field record. This is why the paper recommends a phased, pilot-first approach.

Who supports the system at 3 a.m. when something fails?

The same kind of party that supports it today: a system integrator and the component suppliers, under a support contract. The difference is that support is no longer locked to a single proprietary vendor. With an open architecture the operator can hold a vendor-neutral integrator accountable for the whole system and can change that relationship over time without replacing the control system. Support should be specified and contracted explicitly, exactly as it is for a DCS or PLC today.

What happens if one of the component suppliers goes out of business or exits the market?

This is precisely the risk OPA is designed to reduce. Because components conform to a common standard, a node or application from a departed supplier can be replaced by a conforming product from another supplier without re-engineering the surrounding system. Under the traditional model, the same event forces a far more disruptive and expensive migration.

How is O-PAS different from a vendor telling me their system is already 'open'?

Almost every vendor uses the word 'open,' usually to mean their system speaks a common protocol at the edges while remaining proprietary at the controller and I/O layer. O-PAS is a specific, published standard with a conformance program, covering interoperability, configuration portability, and application portability. The practical test is to ask which of those three properties a product actually delivers and to require evidence of conformance rather than a marketing claim (see Appendix C for specification language).

Do we have to replace everything at once?

No. OPA components interoperate with existing SCADA and, through standard connectivity, with parts of the legacy system, so the transition can be gradual and can span multiple capital cycles. The recommended entry point is an asset already scheduled for replacement, or a bounded pilot, not a plant-wide rip-and-replace.

Is it secure enough for critical energy infrastructure?

Security is built into the standard: O-PAS mandates conformance to the ISA/IEC 62443 cybersecurity series and provides third-party verification through ISASecure. That does not make any given deployment automatically secure, which still depends on correct implementation and operations, but it raises the floor and makes conformance verifiable, which matters for a regulated critical-infrastructure operator.

We are a smaller or independent refiner. Is this only for supermajor-scale sites?

No. Because control is distributed across small, comparatively low-cost conforming nodes, the architecture scales from a single package unit up to a full complex, and does not depend on supermajor scale. For any operator, standardizing interfaces across units and sites is one of the strongest sources of value.

What is the catch? Where is OPA genuinely weaker today?

Two honest weaknesses. First, near-term integration cost currently offsets much of the hardware saving, so early-project savings are modest even though lifecycle savings are large. Second, the total number of at-scale deployments industry-wide is still limited, so an operator cannot yet point to a long list of directly comparable references. Both are manageable, and both are expected to improve as the ecosystem matures, but they are real and are the reason for a measured, evidence-driven rollout.

Appendix B. Glossary of Terms and Acronyms

Brief, working definitions of the terms used in this paper. They are intended for orientation, not as formal standard definitions.

Term	Definition
ACP	Advanced Computing Platform. Standard computing hardware in an OPA system on which applications (control, analytics, historian) run, rather than being locked inside a proprietary controller.
APC	Advanced Process Control. Model-based control (often MPC) layered on the base control system to optimize yield, energy, and throughput; a major source of refining margin.
DCS	Distributed Control System. An integrated, single-vendor platform that controls a continuous process as a coordinated whole; the backbone of refinery and petrochemical unit control.
DCN	Distributed Control Node. The standard building block of control in an OPA system: a compact, low-cost compute element that performs control, connects to I/O, and speaks the standard interfaces.
FCC	Fluid Catalytic Cracking. A primary refinery conversion unit; a common target for advanced process control.
HMI	Human-Machine Interface. The operator's screens and controls.
I/O	Input/Output. The signals and modules that connect a controller to field sensors and actuators.
IEC 61131 / 61499	International standards for control programming. O-PAS supports both; 61499 targets distributed, event-driven control.
ISA/IEC 62443	The international series of standards for the cybersecurity of industrial automation and control systems. Conformance is mandated by O-PAS.
ISASecure	The third-party certification scheme for ISA/IEC 62443; named by OPAF as the exclusive verifier of O-PAS cybersecurity requirements.
MPC	Model Predictive Control. An advanced control technique that optimizes a process against a model; used for energy and efficiency gains.
O-PAS	The Open Process Automation Standard, published by The Open Group. The technical definition of an open, interoperable, secure process control architecture.
OCF	O-PAS Connectivity Framework. The standardized, OPC UA-based connectivity backbone through which all conforming components communicate.
OPA	Open Process Automation. The overall approach of building control systems from interoperable, standards-based components.
OPAF / The Open Group	The Open Process Automation Forum, part of The Open Group, the vendor-neutral body that develops and maintains the O-PAS Standard.
OPC UA	OPC Unified Architecture. The widely adopted industrial interoperability standard on which the OCF is built.
OT	Operational Technology. The hardware and software that monitors and controls physical processes, as distinct from enterprise IT.
PLC	Programmable Logic Controller. A rugged, widely used industrial controller; in refineries, common on package units, compressors, and skids.
PSM / RMP	OSHA Process Safety Management (29 CFR 1910.119) and EPA Risk Management Program (40 CFR 68). Regulations governing the safe management of highly hazardous processes, including management of change.

Term	Definition
SIS	Safety Instrumented System. An independent system, built to IEC 61511 / ISA 84, that takes a hazardous process to a safe state; typically separate from the DCS.
SCADA	Supervisory Control and Data Acquisition. The software layer providing operator screens, alarming, historian, and telemetry across a distributed system.
TSA Security Directives	US Transportation Security Administration cybersecurity directives for pipelines, issued after the 2021 Colonial Pipeline incident and pursued toward permanent rulemaking.
TCO	Total Cost of Ownership. The full lifecycle cost of a system, including capital, maintenance, migrations, and downtime, not just installed price.
Turnaround	A planned, scheduled shutdown of a unit or plant for maintenance and upgrades; the window in which major control-system work is typically done.

Appendix C. Procurement Specification Language

An open architecture stays open only if procurement keeps it open. The clauses below are drafting starting points an operator can adapt into a specification, request for proposal, or contract to ensure that an 'open' procurement is genuinely open, portable, secure, and free of hidden lock-in. They are written to be edited: bracketed items are placeholders, and the Owner should tailor them, with procurement and legal counsel, to the project and jurisdiction.

> **Not legal advice**
> These are illustrative drafting aids, not legal or contractual language for use as-is. Have qualified procurement and legal professionals adapt and review them, and confirm the current O-PAS version and conformance program with The Open Group before citing specific requirements.

1. **Standards conformance.** The control system shall conform to the current published version of the O-PAS Standard. The Supplier shall state the O-PAS version and parts to which each component conforms and shall provide evidence of conformance through The Open Group's conformance program where such certification is available.
2. **Interoperability.** All controllers, distributed control nodes, input/output, applications, and supervisory components shall interoperate through the O-PAS Connectivity Framework using OPC UA. No proprietary protocol shall be required for interoperation among components of the system.
3. **Configuration portability.** System configuration shall be delivered in the standard, portable form defined by the O-PAS information and exchange models, such that the Owner can read, modify, and migrate the configuration without dependence on any single Supplier's proprietary engineering tool.
4. **Application portability.** Control applications shall be portable to any conforming platform. The Supplier shall deliver application definitions in the standard form and shall place no technical or contractual encumbrance on their migration to another conforming Supplier's platform.
5. **Cybersecurity.** Components shall conform to the applicable ISA/IEC 62443 requirements and, where available, shall carry ISASecure certification. The Supplier shall provide certification evidence and shall support the Owner's Risk and Resilience Assessment and Emergency Response Plan obligations.
6. **Multi-vendor sourcing.** The architecture shall allow the Owner to procure conforming replacement or additional components from any qualified Supplier over the system's life, without re-engineering the surrounding system, and the Supplier shall not condition warranty or support on sole-source procurement.
7. **Documentation and ownership.** The Owner shall own, and shall receive complete documentation for, all configuration and application artifacts. Interfaces shall be documented to the standard so that the Owner is not dependent on the Supplier for routine configuration changes.
8. **Obsolescence and lifecycle.** The Supplier shall support component-level replacement across a [25]-year design life and shall not condition continued operation, patching, or expansion on migration to a proprietary successor platform.
9. **Conformance evidence and acceptance.** Acceptance shall be contingent on demonstrated conformance to the standards, security, and portability requirements above, verified during factory and site acceptance testing, and shall not rest on Supplier assertion alone.

About Collaborative Systems Integration

Collaborative Systems Integration (CSI) is a vendor-neutral systems integrator focused on Open Process Automation and the migration of legacy DCS and PLC control systems to open, standards-based architectures. CSI's leadership includes practitioners who helped shape the Open Process Automation movement and who have delivered large control-system programs in industries where downtime is measured in millions of dollars. CSI's role is to help end users evaluate, specify, and implement open architectures on their own terms, capturing the interoperability, portability, cybersecurity, and lifecycle-cost advantages of the O-PAS Standard while managing the practical risks of early adoption.

CSI also publishes on the subject. Trevor Cusworth, CSI's VP of Sales and Marketing, is the author of *Open Process Automation: Architecture*, *Execution & Transformation*, a practitioner's treatment of open control architecture, and CSI produces the flagship *State of Open Process Automation* report, whose 2026 edition assesses the standard, suppliers, integrators, economics, and project-execution practices in a single 40-page industry review.

To learn more or to discuss an obsolescence or migration decision, contact Collaborative Systems Integration. Related resources: the OPA lifecycle-cost (ROI) calculator (csi-automation.com/opa-roi-calculator), CSI Academy training (csi-automation.com/academy), the OPA Community (OPAcommunity.com), and CSI's OPA materials at csi-automation.com.

References and Further Reading

The sources below informed the factual claims in this paper. Figures attributed to a specific organization in the text should be verified against the primary source before use in a formal business case. Standard versions and certification programs continue to evolve; confirm current status with The Open Group.

1. **Collaborative Systems Integration.** State of Open Process Automation 2026: a 40-page industry assessment of the standard, suppliers, integrators, economics, and project execution (published May 31, 2026). *csi-automation.com/state-of-opa-2026*
2. **Cusworth, Trevor.** Open Process Automation: Architecture, Execution & Transformation (book; available via Amazon). *us.amazon.com (search title or ASIN B0H3WD9WHR)*
3. **Collaborative Systems Integration.** OPA lifecycle-cost (ROI) calculator: model hardware, integration, and 25-year ownership cost for your own I/O count and site topology. *csi-automation.com/opa-roi-calculator*
4. **CSI Academy.** Open Process Automation training courses for engineering and operations staff. *csi-automation.com/academy*
5. **The Open Group, Open Process Automation Forum.** O-PAS Standard, publications and forum pages. *opengroup.org/forum/open-process-automation-forum ; pubs.opengroup.org/open-process-automation*
6. **Architecture & Governance Magazine.** The Open Group Open Process Automation Forum Publishes the O-PAS Version 2.1 Preliminary Standard. *architectureandgovernance.com*
7. **Control Engineering.** New cost analysis: Open process automation saves 52% versus DCS (reporting on the COPA analysis presented by Don Bartusiak, CSI, at the 2024 ARC Industry Forum). *controleng.com*
8. **ISA / ISASecure.** The Open Group Open Process Automation Forum (OPAF) Selects ISASecure as Exclusive Verification Provider for Cybersecurity Requirements in the O-PAS Standard (August 2024). *isa.org*
9. **Automation.com.** Open Automation Systems: Update on the State of the Art (September 2024), incl. ExxonMobil Lighthouse project and OPAF membership. *automation.com*
10. **OPC Foundation / OPC Connect.** Achieving Interoperability for Process Automation Systems (DCN, OCF, OPC UA, version timeline). *opcconnect.opcfoundation.org*
11. **ARC Advisory Group.** ExxonMobil's Open Process Automation Lighthouse: lessons from a live O-PAS deployment (Baton Rouge Resins Finishing Plant, cutover end of 2024). *arcweb.com*
12. **OSHA / EPA / TSA (primary sources).** OSHA Process Safety Management (29 CFR 1910.119); EPA Risk Management Program (40 CFR 68); TSA pipeline security directives (confirm current status). *osha.gov ; epa.gov ; tsa.gov*