COLLABORATIVE SYSTEMS INTEGRATION

WHITE PAPER · PROCESS CONTROL ARCHITECTURE

Open Process Automation for Power Generation

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 power generation 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. Power generation shares the continuous, capital-intensive character of those industries, so the figures are a reasonable directional guide rather than a validated power-sector number, and each reflects the specific study and plant it came from. This paper flags where a figure should not be generalized to a power station. 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

Power plants run some of the largest and longest-lived control systems in any industry. It is common to find turbine controls, a boiler and balance-of-plant distributed control system (DCS), programmable logic controllers on auxiliaries, and a separate protection and safety system, each from a different supplier and specified twenty or thirty years ago, now approaching or past the end of its supported life. Because these platforms are proprietary, the generator's freedom to modernize is limited by a single supplier's roadmap, spare-parts availability, and pricing. Replacing a control system is expensive, has to be squeezed into a planned outage, 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 power generation: proprietary turbine and DCS platforms reaching end of life, a mandatory and tightening cybersecurity regime, and the need to integrate renewables and storage into plants built for none of it. The architecture and the industry's pain points line up well, with the honest qualifier that OPA has not yet been proven at scale in a power station.

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, not a power station, but power generation is continuous and capital-intensive enough that they are a reasonable directional guide; each generator 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 a generator 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.** OPA has been proven in the field, but not in power. The flagship deployment is ExxonMobil's OPA Lighthouse at its Baton Rouge petrochemical plant, which cut over at the end of 2024 and has since run a live production unit. There is no public, at-scale deployment in power generation yet, so a generator adopting now is an early adopter, though the mandatory NERC CIP cybersecurity regime is one place where an architecture with security specified in has an unusually clear advantage.

This paper explains what OPA is, characterizes how it differs from PLC and DCS approaches, compares the three on the dimensions that matter to a generator, maps concrete power generation 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 Power Generation

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

2.1 A layered patchwork, assembled over decades

A typical power plant does not run one control system. It runs several, layered and stitched together over many outage and capital cycles. The turbine, gas or steam, is controlled by a proprietary turbine-control system from its original equipment manufacturer. The boiler and balance of plant run on a distributed control system, often from a different vendor. Auxiliaries such as fuel, water, and air handling run on their own PLCs. A separate protection and safety system handles trips and interlocks. A historian and plant controls 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 outage window, and the knowledge of how it all fits together often lives in a small number of long-tenured engineers and integrators.

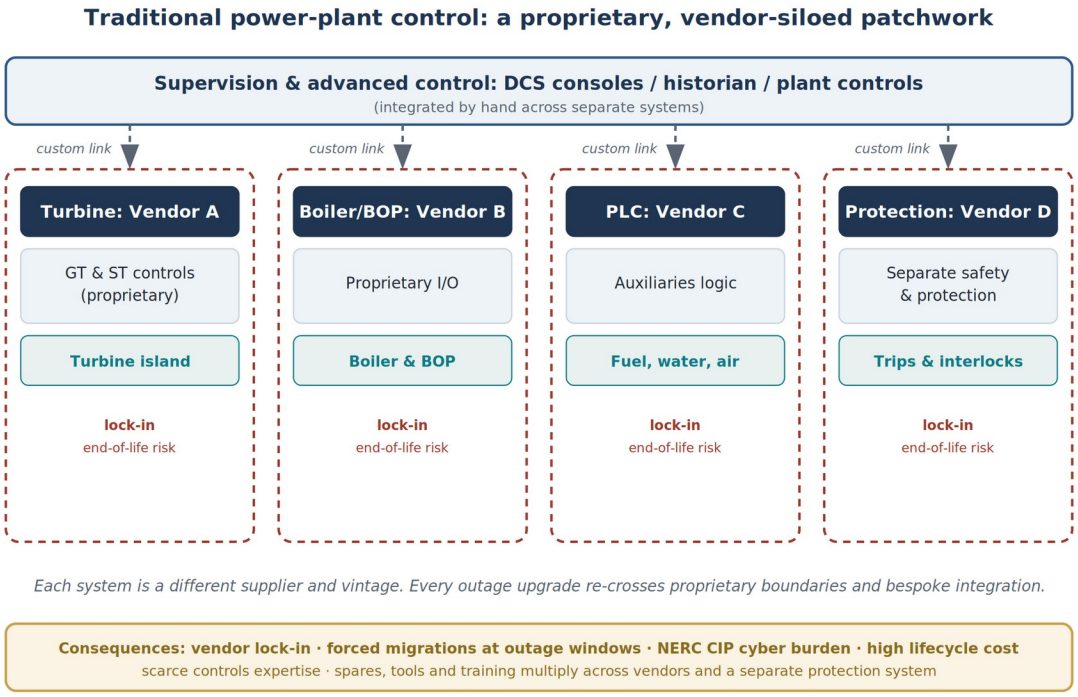

Figure 1. *The traditional power-plant control estate is a set of proprietary, vendor-specific silos, turbine controls, a boiler and balance-of-plant DCS, auxiliary PLCs, and a separate protection system, stitched together by hand. Each silo carries its own lock-in and end-of-life risk.*

2.2 Aging infrastructure and obsolescence

The installed base is old. Many power plant 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 outage. 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

Power generation is the archetypal critical infrastructure, and it is the one sector in this series with a mandatory, enforceable cybersecurity regime: the NERC Critical Infrastructure Protection (CIP) standards, backed by financial penalties. The threat is not hypothetical; the 2015 and 2016 attacks on the Ukrainian grid showed that control systems can be reached and operated by adversaries. Older control systems were designed for isolated networks and often predate modern security expectations, yet they are increasingly connected for remote operations, analytics, and enterprise integration. Retrofitting the segmentation, access control, patching, and monitoring that NERC CIP expects onto architectures never designed for them is difficult and expensive. Generators need security 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 Turbine controls and protection live in separate silos

Two of the most important layers in a power plant, the turbine-control system and the protection and safety system, typically sit outside the DCS as separate, proprietary systems with their own engineering environments. Turbine controls in particular are closely held by the original equipment manufacturer and are among the most locked-in systems in the plant. Each is a separate vendor relationship, a separate lifecycle, and a separate integration to maintain. An architecture that provides standard interfaces lets these layers connect in a consistent, documented way and lets control and optimization applications move forward rather than being rebuilt each cycle.

2.7 Regulatory pressure is rising

Power generation operates under a dense regulatory framework, and the parts that touch control systems are tightening, not relaxing. Cybersecurity is governed by the NERC Critical Infrastructure Protection standards, mandatory reliability standards enforced by NERC under FERC oversight, with financial penalties for non-compliance, covering asset identification, access control, systems security, incident response, and, under CIP-013, supply-chain risk. Emissions and reliability rules add further pressure to modernize ageing plants. Unlike most sectors, cybersecurity here is not aspirational: it is audited and enforced, which makes an architecture that specifies ISA/IEC

62443 conformance and can evidence it through third-party certification directly useful for demonstrating and sustaining CIP compliance.

The direction of travel is clear: the reliability and security expectations on the bulk power system are becoming more prescriptive, not less. A control architecture with security specified in and documented, standard interfaces is aligned with where NERC and FERC are heading rather than fighting it. *(NERC CIP standards are revised on a regular cycle and requirements change; generators should confirm the current CIP version and applicability with their compliance function and regional entity.)*

2.8 The economics are driven by availability and forced outages

A power plant's economics are driven by availability: every hour the unit cannot generate is lost revenue, and on a plant that sets or follows the market price the value of an avoided forced outage is large. Control-system reliability and cyber-resilience are therefore a direct commercial issue, and a NERC CIP violation carries its own financial penalty. Major control-system work is generally constrained to planned outages that come only every year or few years, so the timing of an obsolescence-driven migration matters enormously. For regulated utilities, control-system capital typically enters the rate base, which rewards prudent, well-justified investment; for merchant plants it competes directly with generation margin. In both cases the open architecture's promise is a lower lifecycle cost and a migration that can be done in pieces at successive outages rather than as one forced forklift. *(The value of availability varies widely by plant type, market, and dispatch position; generators should use their own 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.

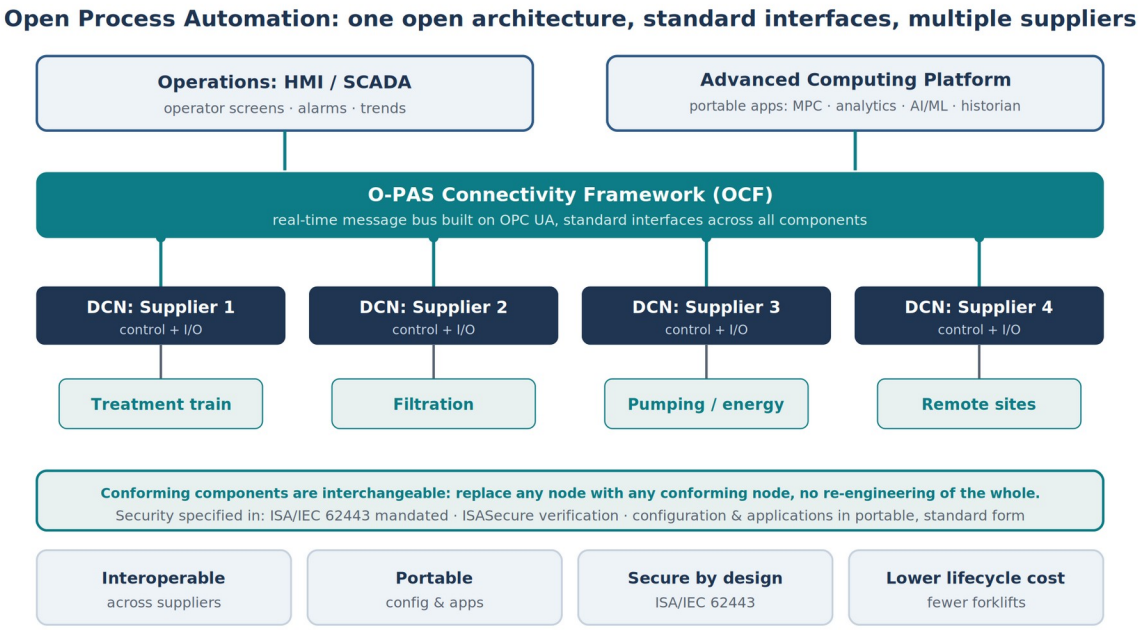

Figure 2. *In an OPA system, conforming components from multiple suppliers connect through the OPC UA-based O-PAS Connectivity Framework. Distributed Control Nodes, applications, and supervision all share standard interfaces, so any conforming component can be replaced without re-engineering the whole.*

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.

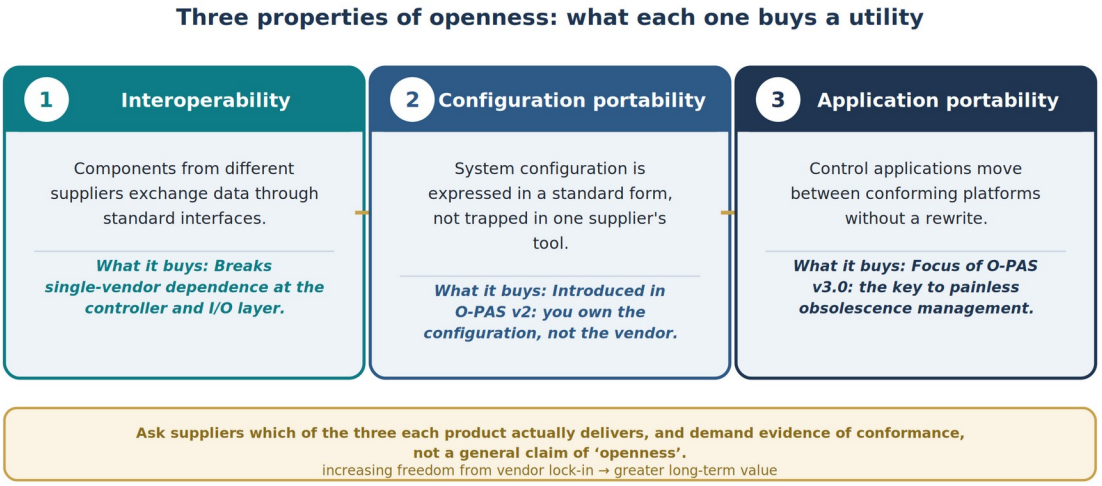

Figure 3. *Interoperability, configuration portability, and application portability are distinct properties. A product can deliver one without the others, so an operator should ask specifically which it provides and require evidence of conformance.*

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 power generation, 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, power plants 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 power generator 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 power generation	High; the sector backbone	High; on auxiliaries	Proven in other sectors; not yet at scale in power

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 power 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 generating fleet, 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), not from power generation, but power is continuous and capital-intensive enough that they are a reasonable directional guide; still, they reflect a specific modeled plant and specific assumptions. They indicate 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 plant's own I/O count and 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 Power Generation

The abstract advantages become concrete when mapped to the situations power generators 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 Outage-aligned control modernization

A turbine control or DCS at end of support faces a forced migration, and that migration has to happen during a planned outage. This is the natural entry point for OPA, because the generator 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 generator spends similar money but buys future optionality instead of another proprietary cycle, and can demonstrate the security posture the migration establishes against NERC CIP.

6.2 Standardizing across a generating fleet

A generating fleet accumulates a mix of turbine controls, DCS, and PLC platforms from many projects, vendors, and eras. Adopting a common set of standard interfaces across new and refreshed units lets the operator reduce the number of distinct platforms it must stock spares for, train staff on, secure, and integrate. A consistent connectivity and security model across the fleet also simplifies NERC CIP compliance, which is far easier to demonstrate on a standardized estate than on a patchwork.

6.3 Adding advanced control and optimization

Power plants have real efficiency and flexibility headroom, in heat-rate optimization, combustion and emissions control, and, increasingly, in integrating renewables, batteries, and hydrogen co-firing into plants that were never designed for them. Each such application is, in a closed system, a custom proprietary integration rebuilt at every migration. OPA's model of portable applications running on standard compute platforms makes it materially easier to add advanced control and to integrate new generation and storage assets, and to carry those applications forward as the control hardware is refreshed rather than rebuilding them each time.

6.4 Enterprise-wide architecture across the fleet

An operator running several stations benefits from a single architectural standard across all of them: common interfaces, common security controls, transferable staff skills, and consolidated spares. Because every conforming component connects through documented standard interfaces, security and data flows are consistent across the fleet, which supports the auditable, standardized posture NERC CIP rewards. OPA provides that standardization without forcing every station onto identical hardware.

> **A realistic note on adoption**
>
> OPA has been proven in the field in oil, gas, and chemicals, most visibly ExxonMobil's Lighthouse at its Baton Rouge petrochemical plant, but there is no public, at-scale deployment in power generation yet. A generator adopting OPA now is a genuine early adopter, and the interaction with NERC CIP compliance has to be worked through deliberately. That said, the fit is strong, and it argues for the phased, pilot-first approach described in the next section: prove it first on a non-critical balance-of-plant system.

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.

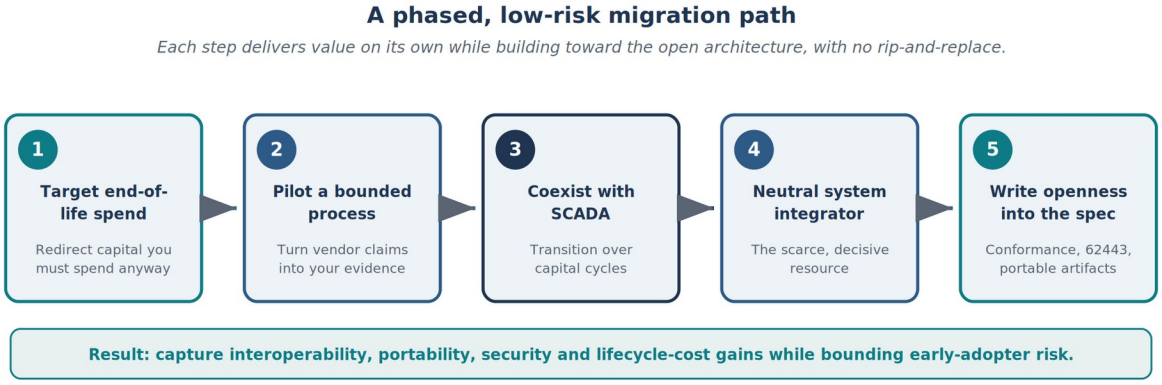

Figure 4. *A phased path lets an operator adopt OPA where obsolescence is already forcing spend, prove it on a bounded pilot, and expand through coexistence, rather than a single high-risk replacement.*

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 outage, 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 outage 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

Power generators carry a control system for two or three decades, and availability, not installed cost, is what pays for the plant. That makes lifecycle cost, and the reliability and compliance the system supports across that life, the right frame, and it is the frame in which OPA's argument is strongest.

8.1 Capital versus lifecycle

The evidence comes from continuous-process industries rather than power, 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 downtime cost was included, a figure that resonates in a power plant where every hour of forced outage is lost generation.

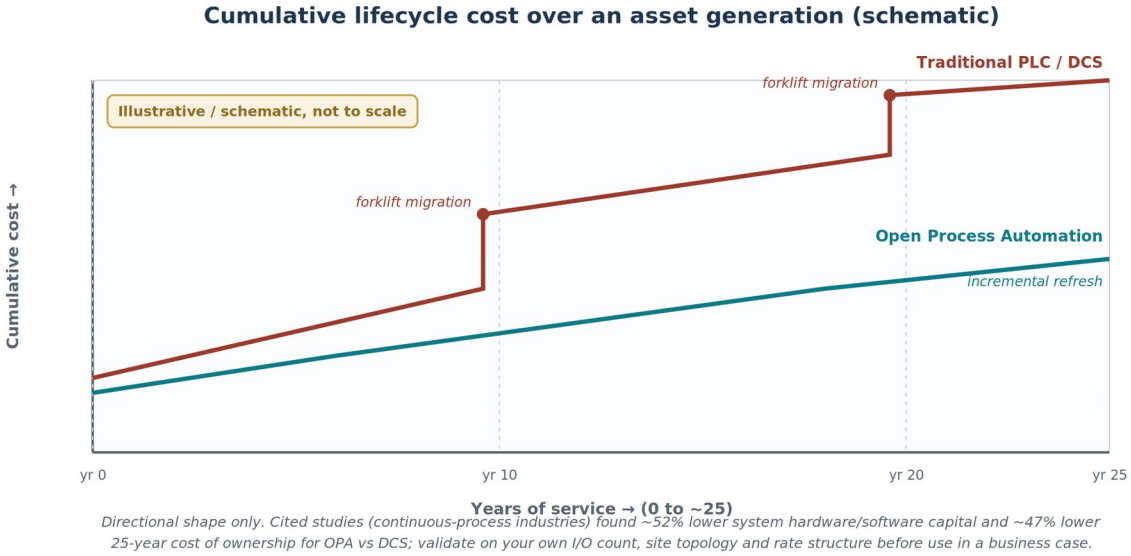

Figure 5. *Schematic of cumulative lifecycle cost. Traditional systems step up at each forced forklift migration; an open architecture is refreshed incrementally. Shape is illustrative only; the cited savings come from continuous-process studies and should be re-derived on an operator's own numbers.*

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 power generator should weigh, stated plainly.

- **No power-sector field references yet.** OPA has been proven in oil, gas, and chemicals, but there is no public, at-scale deployment in power generation. A generator adopting now is an early adopter with no directly comparable power reference to point to.
- **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 and compliance models lag.** Utility capital planning, frame agreements, and NERC CIP compliance processes are built around traditional single-vendor systems. Multi-vendor, standards-based sourcing may require adapting specification, evaluation, contracting, and the compliance evidence base.

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

Power generators are, more than most industries, hostage to the longevity and closure of their control systems. They run ageing, proprietary, layered systems, turbine controls, DCS, and protection, on critical infrastructure, they are pushed to modernize for reliability, a mandatory cybersecurity regime, and the integration of new generation, 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 the process industries 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 power generation's problems is strong, and the security-by-design that O-PAS mandates lands especially well against a mandatory NERC CIP regime. The honest qualifier is maturity: OPA has not yet been proven at scale in a power station, near-term integration costs still offset much of the hardware saving, and the interaction with CIP compliance has to be built deliberately. But the strategic direction is clear, and the risk is manageable through a phased, pilot-first approach. For a generator making a decades-long commitment on a station, 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 power generation 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?

The standard is real and published, conformant products exist, and it has been proven in the field: ExxonMobil's Lighthouse has run a live unit at its Baton Rouge petrochemical plant since the end of 2024. What does not yet exist is a public, at-scale deployment in power generation. So in power it is proven as an architecture but not yet in a generating station, which is why the paper recommends starting on a non-critical system and working through the NERC CIP implications deliberately.

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.

How does this fit with NERC CIP compliance?

It fits unusually well. NERC CIP is a mandatory, enforced regime, and O-PAS mandates ISA/IEC 62443 conformance with third-party verification through ISASecure, so security is specified into the architecture and can be evidenced rather than asserted. A standardized, documented, multi-vendor estate is generally easier to secure and to audit than a patchwork of proprietary systems. The CIP compliance approach still has to be worked through with your compliance function up front; the architecture is designed to make that easier, not to replace it.

We run a small fleet or a single station. Is this only for large utilities?

No. Because control is distributed across small, comparatively low-cost conforming nodes, the architecture scales from a single balance-of-plant system up to a multi-station fleet, and does not depend on the scale of a large utility. For any generator, standardizing interfaces and security across units 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 layered on the base control system to optimize heat rate, combustion, and emissions in a power plant.
DCS	Distributed Control System. An integrated, single-vendor platform that controls a process as a coordinated whole; the backbone of boiler and balance-of-plant control in a power station.
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.
BOP	Balance of Plant. The auxiliary systems around the boiler and turbine, fuel, water, air, and emissions handling.
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 power plants, common on auxiliaries and balance-of-plant systems.
NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection standards. Mandatory, enforceable cybersecurity standards for the bulk electric system, overseen by FERC.

Term	Definition
Protection system	The independent protection and safety system that trips a generating unit and enforces interlocks; 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.
FERC	US Federal Energy Regulatory Commission. Oversees NERC and the mandatory reliability standards, including NERC CIP, for the bulk power system.
TCO	Total Cost of Ownership. The full lifecycle cost of a system, including capital, maintenance, migrations, and downtime, not just installed price.
Outage	A planned, scheduled shutdown of a generating unit 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 and NERC CIP.** 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 NERC CIP compliance obligations, including asset identification, access control, systems security, and audit evidence.
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. **NERC / FERC (primary sources).** NERC Critical Infrastructure Protection (CIP) reliability standards; FERC reliability oversight (confirm current CIP version and applicability). *nerc.com ; ferc.gov*

Disclaimer: This white paper is provided for informational purposes. It does not constitute engineering, financial, or legal advice. Cost and performance figures cited from third-party analyses reflect the conditions and assumptions of those analyses and may not transfer directly to a specific facility. Readers should validate all figures, current standard versions, and certified-product availability against primary sources before making procurement or investment decisions.