CHEMICAL ENGINEERING
ESSENTIALS FOR THE CPI PROFESSIONAL

Electronically reprinted from January 2023

Open Process Automation is Gaining Sustainable Momentum

Digital transformation in the chemical process industries demands open architecture, enterprise-wide interoperability and a focus on sustainability. Progress discussed here is moving the industry in that direction

Kevin Finnan
Yokogawa

Many companies in the chemical process industries (CPI) are currently pursuing digital transformations to accelerate their business strategies. Enabled by a broad range of digital technologies, such sweeping transformations empower people, optimize processes and automate systems to radically reorient business performance.

In the face of multiple, evolving market dynamics, companies have found that engaging in the digital transformation is necessary to provide the agility to compete and thrive in "new normal" ecosystems. The transformed enterprises can respond more rapidly to new user requirements, supply chain issues and market disruptions.

Achieving the agility and responsiveness that is the hallmark of digital-transformation initiatives often requires merging disciplines that formerly operated in silos. For instance, operations technology (OT) personnel find their organizations requiring tight integration with information technology (IT) staff in newly collaborative, highly data-intensive environments that have deployed real-time analytics, artificial intelligence (AI), cloud- and edge-computing technologies, digital twins and industrtial internet of things (IIoT) tools.

Under pressure to reduce capital and lifecycle costs and improve their profitability, the OT staff has recognized that proprietary technologies present serious obstacles to digital transformations. Closed systems, such as those used for process automation, are expensive to upgrade and maintain. Upgrades can also be risky. Many operations forego migrating or refreshing their technology in order to avoid the risk of prolonged downtime. As the system ages, other risks increase. These include hardware failures and changes in technology that prevent replacement.

There is another risk that cybersecurity cannot be updated to safely protect operations, assets and capital investments. Legacy systems become more challenging to integrate with current or future best-in-class technologies, such as those required to digitally transform. Digital transformations demand enterprise-wide interoperability, cybersecurity, agility and sustainability. Networks with customized integration that connect formerly siloed, proprietary systems are expensive, hard to utilize and hence become unsustainable.

The "great crew change" and the incoming workforce that tends to be younger and more computer-knowledgeable are always key enablers for digital transformations. Digital transformation program teams have found that technically savvy newcomers, who are accustomed to interoperable consumer products, take a very dim view of closed, proprietary systems in the workplace.

In light of this situation, the Open Process Automation Forum (OPAF) of the Open Group (www.opengroup.org) began working in 2016 to develop a set of Open Process Automation Standards (O-PAS). The Open Group is a global consortium that helps organizations achieve business objectives through technology standards. OPAF is an international forum of end users, system integrators, suppliers, academia and standards organizations working together to develop a standards-based, open, secure and interoperable process automation architecture. An open architecture and interoperability supported by industry standards provide a solid and necessary path forward for digital transformations leading to system sustainability.

'Standard of standards'

OPAF's open process automation "standard of standards" ensures that future automation systems adopt and reinforce standards that achieve true interoperability of hardware and software while also providing built-in security, future-proof innovation and greatly simplified migration. These will enable end-users to realize much more value from their operations.

The idea of a standard of standards is the result of OPAF's effort to leverage work already accomplished by a broad variety of organizations. Industry standards reflect an industry-wide consensus and form a solid, sustainable foundation for open systems. Therefore, wherever possible, O-PAS references existing standards from the most well-established, global organizations — those standards that are most likely to endure in the long term.

To close the gaps, OPAF has been working with the appropriate groups to update their standards or incorporate O-PAS requirements. OPAF has established liaisons with organizations such as the Control System Integrators Association (CSIA), Industrial Internet Consortium (IIC), International Society of Automation (ISA), NAMUR and the OPC Foundation.

Global standards are referenced throughout O-PAS. The technical architecture is based on IEC 62264 (ISA-95), alarm management on IEC 62862 (ISA-18.2), and integral cybersecurity on IEC 62443 (ISA-99). OPAF is also in discussions with the ISA Security Compliance Institute (ISCI) as an ISA/IEC 62443 validation authority.

O-PAS incorporates IEC 61131-3 function blocks, IEC 61499 event-based programming, IEC 62714 (AutomationML) for control applications, and DMTF Redfish for systems management. The connectivity framework, information and exchange models are based on IEC 62541 (OPC UA). Notably, the OPC Foundation has taken a step beyond the liaison agreement by joining OPAF as a member.

The benefits of standards deployment are far-reaching. The latest O-PAS version tightly defines and controls system data and requires uniform alarm reporting. Yokogawa's Dave Emerson, who is co-chair of OPAF's Enterprise Architecture Working Group, explains it by saying that in the past, each supplier used to publish alarms and event conditions in different formats, so users had to waste time with different types of messages. Now, consistent reporting means they can save time.

Scope and vision

O-PAS enables the development of systems composed of cohesive, loosely coupled, severable functional elements from independent suppliers. The elements are easily integrated via a structured modular architecture. O-PAS does not define the functional intellectual property (IP) in the products; the IP can remain proprietary to their suppliers. Instead, the objective is to define open standard interfaces. Interoperability is the key.

As shown in Figure 1, the O-PAS scope encompasses today's distributed control systems (DCS) and programmable logic controllers (PLC) for continuous and hybrid process industries. Out-of-scope are business systems and communication protocols between the input-output (I/O) and field instruments. OPAF also decided that safety instrumented systems (SIS) would be out-of-scope because there must be separate and independent combinations of sensors, logic solvers and final elements to achieve required safety integrity levels per the ISA84 and IEC 61511 standards.

An Open Process Automation (OPA) system is a software-defined control system. It is an open system with all the benefits of a traditional DCS or PLC system and more — but without the limitations resulting from supplier hardware or software locking. End-users or integrators can design, operate and expand functions with a wide range of interoperable software and hardware capabilities from multiple suppliers and technologies.

By decoupling hardware and software and employing a service-oriented architecture, the necessary software functions can be situated in many different locations or processors. Not only can software applications run in most hardware, but they can also access any I/O to increase flexibility when designing a system.

Figure 2 shows a reference OPA architecture with O-PAS-compliant products and non-compliant or legacy products. A realistic scenario for many end-users is to "start small," using a hybrid system with a combination of OPA and proprietary components, followed by a steady transition from the legacy system to one that is completely open, interoperable and sustainable.

In an OPA system, most applications and workloads are containerized to run flexibly and in an interoperable manner, utilizing the O-PAS Communication Framework (OCF). The OCF provides a secure, standardized interconnection between O-PAS-compliant software functions. Based on the OPC Unified Architecture (UA), the OCF provides protected, standards-based, reliable data transport.

The distributed control node (DCN) is considered the fundamental O-PAS building block. An edge device, it is a scalable controller, I/O or gateway device that can handle I/O and computing functions. Since hardware and control software are decoupled, the exact function of a particular DCN is up to the system architect. A DCN consists of hardware and system software that enables it to communicate on the OCF and run control software. A DCN can be hardware or virtual. A system can use a few or several thousand DCNs.

Device suppliers are allowing end-users to add, configure and program the software components of the hardware devices based on their requirements. In order to make the device visible as a DCN to the rest of the system, the O-PAS Communication Interface (OCI) software layer can be added as an embedded application to any such non-compliant, flexible architecture-based device.

The advanced computing platform (ACP) enables DCN functionality, but includes scalable computing components, such as CPU cores, memory and storage media to handle applications that require more resources than are typically available in a DCN. ACPs may also be used for applications that cannot be easily or efficiently distributed. ACPs can be on-premise servers or in a cloud

Gaining momentum

O-PAS is gaining momentum on a daily basis. Don Bartusiak, co-chair of OPAF and president of Collaborative Systems Integration has reported that OPAF has 110 organization members, as of the beginning of 2023, including 22 operating companies, six of the major DCS suppliers, and a host of other suppliers and system integrators.

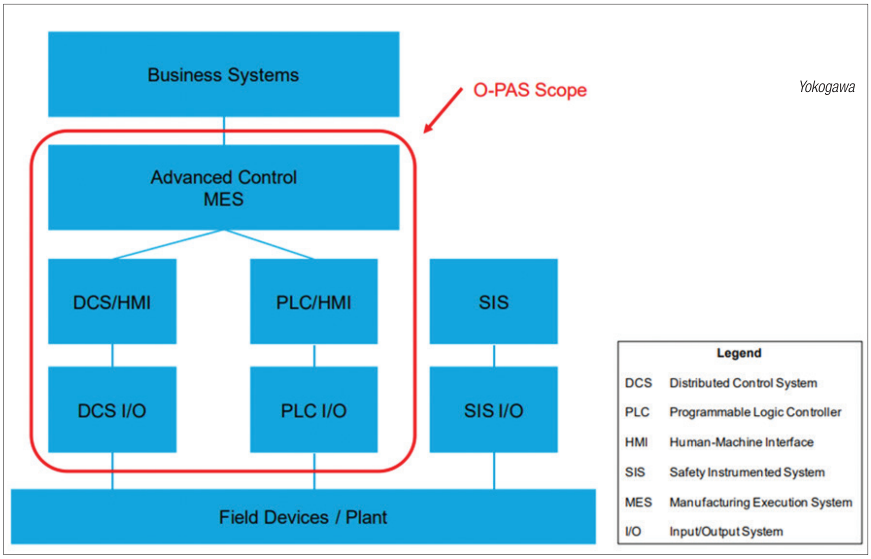
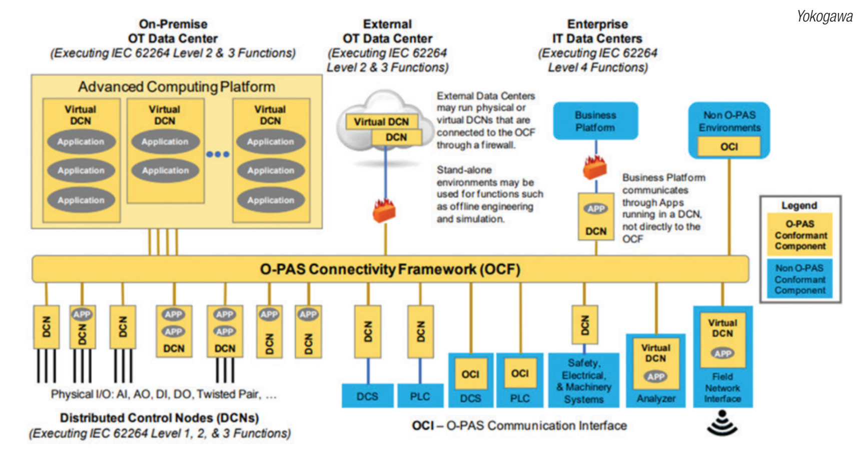

Business Systems
O-PAS Scope
Yokogawa
Advanced Control
MES
DCS/HMI
PLC/HMI
SIS
DCS I/O
PLC I/O
SIS I/O
Field Devices / Plant
Legend
DCS Distributed Control System
PLC Programmable Logic Controller
HMI Human-Machine Interface
SIS Safety Instrumented System
MES Manufacturing Execution System
I/O Input/Output System

FIGURE 1. The scope of the O-PAS includes the DCS, PLC and manufacturing execution system. Business systems, safety instrumented systems and field devices are outside the O-PAS scope


On-Premise
OT Data Center
(Executing IEC 62264 Level 2 & 3 Functions)
External
OT Data Center
(Executing IEC 62264 Level 2 & 3 Functions)
Enterprise
IT Data Centers
(Executing IEC 62264 Level 4 Functions)
Advanced Computing Platform
Virtual DCN
Application
Virtual DCN
DCN
External Data Centers may run physical or virtual DCNs that are connected to the OCF through a firewall.
Stand-alone environments may be used for functions such as offline engineering and simulation.
Business Platform
Non O-PAS Environments
OCI
APP
Business Platform communicates through Apps running in a DCN, not directly to the OCF
Legend
O-PAS Conformant Component
Non O-PAS Conformant Component
O-PAS Connectivity Framework (OCF)
DCS
PLC
Safety, Electrical, & Machinery Systems
Analyzer
Field Network Interface
Physical I/O: AI, AO, DI, DO, Twisted Pair, …
Distributed Control Nodes (DCNs)
(Executing IEC 62264 Level 1, 2, & 3 Functions)
OCI – O-PAS Communication Interface

Yokogawa

FIGURE 2. An O-PAS reference architecture shows a hybrid system that consists of O-PAS-compliant products as well as legacy or non-compliant products

There are well-established O-PAS demonstrators and testbeds at BASF, Dow Chemical, and Georgia Pacific, plus testbed collaborations between Aramco and Schneider in the Middle East and ExxonMobil with Yokogawa in The Woodlands, Texas.

In a new development, ExxonMobil has announced a major step beyond its testbed, with an O-PAS field trial in an actual plant process, scheduled for commissioning in 2023. Shell and Petronas also recently announced new testbed projects, while Evonik announced a project with Collaborative Systems Integration.

Bartusiak and OPAF leaders have indicated that several real-world prototype projects are producing vital know-how from which everyone can benefit, especially when they seek to scale up interoperable systems and process applications in the future.

In addition to learning from these projects, which are sponsored by industry-leading companies, there are other ways for smaller prospective users to expedite their involvement. Recently, a number of OPAF-member suppliers and system integrators formed the Coalition for Open Process Automation (COPA). The coalition includes Codesys, CPlane.ai, CSI, Phoenix Contact, Smar, and the University of Western Australia. To advance the starting point for smaller end-users, COPA has developed a "QuickStart" training program for control system interoperability using O-PAS.

Another recent development is the publication, in December 2021, of the O-PAS Business Guide, Version 2.0, which provides a value proposition for O-PAS and describes how prospective participants can formulate a business case.

OPAF envisions a business ecosystem of end-users, system integrators, hardware and software product suppliers, and solution and service providers. Roles and responsibilities are defined for procurement, design, development, integration, deployment, operation and sustainment of O-PAS-certified products. A company can perform one or more roles in the ecosystem. OPAF also defines how the business models of current stakeholders will be impacted by OPA interoperability.

Pushback from system suppliers who might consider OPA a threat to their proprietary IP has been mild. After all, automation suppliers are not dinosaurs stuck in the 1970s. They have opened up their architectures with commercial off-the-shelf (COTS) hardware and software such as Microsoft Windows, broad communication support such as Ethernet and field device networks, and virtualized platforms.

Still, significant proprietary content remains. Manufacturers who must be agile, responsive and innovative to compete on a daily basis in emerging business ecosystems consider that risky. Also, despite a highly regarded track record in terms of user responsiveness, dependence on closed system suppliers is considered risky in markets requiring agility.

Proprietary system upgrades are expensive, and even in a case where a system supplier offers a great deal in one instance, the risk still exists that the next upgrade will be expensive. And the downtime risk still remains, as well. Although a recent partnership between a major offshore oil producer and a leading automation company recently accomplished a broad technology refresh with no downtime, this type of feat is considered very innovative. Open architecture will allow the "no downtime technology refresh" to be the standard practice.

Concerns have been raised that OPA could undermine the main automation contractor (MAC) concept, in which major system suppliers offer the advantage of deep knowledge of their own products. But the MAC concept has evolved significantly beyond that. Recent MAC projects have included third-party content on a large scale. For example, the author's company has managed procurement, IT and instrumentation ranging from analyzers to valves. Given that sort of experience with proprietary, third-party platforms, it could be easily argued that OPA will greatly simplify project engineering. A broad range of systems integrator companies have agreed with this idea.

Many end-users also feel that open architectures and interoperability are necessary to support the environmental, social and governance (ESG) objectives to which they are striving in pursuit of their sustainability goals. OPA is not a matter of if, it is a matter of when. As OPA becomes mainstream, the vision and capabilities expand and the players in the space gain momentum. Businesses that embrace this technology will adroitly define the industry pivots instead of trying to catch up to them. ■

Edited by Scott Jenkins

Author

Kevin Finnan is a market intelligence and strategy advisor at Yokogawa Corp. of America (12530 West Airport Boulevard, Sugar Land, TX 77478; Email: kevin.finnan@yokogawa.com). Finnan was previously an independent consultant, as well as vice president of marketing for CSE-Semaphore, and director of marketing at Bristol Babcock. He has over 30 years of experience in a variety of vertical markets and has launched more than 40 products in automation and measurement technologies.