The Open Group Preliminary Standard

O-PAS™ Standard, Version 1.0

Part 1 – Technical Architecture Overview (Informative)

The Open Group Preliminary Standard

O-PAS™ Standard, Version 1.0: Part 1 – Technical Architecture Overview (Informative)

Document Number: P190-1

Published by The Open Group, February 2019.

Comments relating to the material contained in this document may be submitted to:

The Open Group, Apex Plaza, Forbury Road, Reading, Berkshire, RG1 1AX, United Kingdom

or by electronic mail to:

ogspecs@opengroup.org

Contents

Preface

The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through technology standards. Our diverse membership of more than 600 organizations includes customers, systems and solutions suppliers, tools vendors, integrators, academics, and consultants across multiple industries.

The mission of The Open Group is to drive the creation of Boundaryless Information Flow™ achieved by:

- Working with customers to capture, understand, and address current and emerging requirements, establish policies, and share best practices
- Working with suppliers, consortia, and standards bodies to develop consensus and facilitate interoperability, to evolve and integrate specifications and open source technologies
- Offering a comprehensive set of services to enhance the operational efficiency of consortia
- Developing and operating the industry's premier certification service and encouraging procurement of certified products

Further information on The Open Group is available at www.opengroup.org.

The Open Group publishes a wide range of technical documentation, most of which is focused on development of Standards and Guides, but which also includes white papers, technical studies, certification and testing documentation, and business titles. Full details and a catalog are available at www.opengroup.org/library.

This Document

This document is Part 1 of the O-PAS™ Standard, Version 1.0, a Preliminary Standard of The Open Group. It has been developed and approved by The Open Group.

The O-PAS Standard consists of the following five parts (of the anticipated eight parts to be published in the full standard):

- O-PAS Part 1 – Technical Architecture Overview (Informative) (this document)
- O-PAS Part 2 – Security (Informative)
- O-PAS Part 3 – Profiles
- O-PAS Part 4 – Connectivity Framework (OCF)
- O-PAS Part 5 – System Management

The parts listed above will each be a separate document that can be updated and re-versioned as required as we move forward with the O-PAS Standard.

The O-PAS Standard, Version 1.0 is being published initially as a Preliminary Standard since it addresses an emerging area of technology; therefore, it may change before being published as a full Standard of The Open Group. In such a case it will be made as upwards-compatible as possible with the corresponding Preliminary Standard, but complete upwards-compatibility is not guaranteed.

Conventions

A Glossary and Abbreviations reference is available. If a term is not defined in that document then the common English definition, as defined in Merriam-Webster's Collegiate Dictionary, applies.

Trademarks

ArchiMate®, DirecNet®, Making Standards Work®, Open O® logo, Open O and Check® Certification logo, OpenPegasus®, Platform 3.0®, The Open Group®, TOGAF®, UNIX®, UNIXWARE®, and the Open Brand X® logo are registered trademarks and Boundaryless Information Flow™, Build with Integrity Buy with Confidence™, Dependability Through Assuredness™, Digital Practitioner Body of Knowledge™, DPBoK™, EMMM™, FACE™, the FACE™ logo, IT4IT™, the IT4IT™ logo, O-DEF™, O-HERA™, O-PAS™, Open FAIR™, Open Platform 3.0™, Open Process Automation™, Open Subsurface Data Universe™, Open Trusted Technology Provider™, Sensor Integration Simplified™, SOSA™, and the SOSA™ logo are trademarks of The Open Group.

Java® is a registered trademark of Oracle Corporation and/or its affiliates.

UML® is a registered trademark of Object Management Group, Inc. in the United States and/or other countries.

All other brands, company, and product names are used for identification purposes only and may be trademarks that are the sole property of their respective owners.

Acknowledgements

The Open Group gratefully acknowledges the International Society of Automation for use of the ISA copyrighted ANSI/ISA 62443 series of standards. Visit www.isa.org.

Referenced Documents

The following documents are referenced in Part 1 of the O-PAS Standard.

The documents are referred to in the text in such a way that some or all of their content constitutes requirements of this part. For dated references, only the version cited applies. For undated references, the latest version of the referenced document (including any amendments) applies.

(Please note that the links below are good at the time of writing but cannot be guaranteed for the future.)

Normative References

Normative references for Part 1 of the O-PAS Standard are defined in Section 1.4.

Informative References

- ANSI/ISA-62443-1-1:2007: Security for Industrial Automation and Control Systems – Part 1-1: Terminology, Concepts, and Models (adopted by IEC as IEC 62443-1-1)
- IEC 61131-3:2013: Programmable Controllers – Part 3: Programming Languages; refer to: https://webstore.iec.ch/publication/4552
- IEC 61499-1:2012: Function Blocks – Part 1: Architecture; refer to: https://webstore.iec.ch/publication/5506
- IEC 61512-1:1997: Batch Control – Part 1: Models and Terminology (ISA 88.00.01); refer to: https://webstore.iec.ch/publication/5528
- IEC 62264-1:2013: Enterprise-Control System Integration – Part 1: Models and Terminology (ISA 95.00.01); refer to: https://www.iso.org/standard/57308.html
- IEC 62264-3:2016: Enterprise-Control System Integration – Part 3: Activity Models of Manufacturing Operations Management (ISA 95.00.03); refer to: https://www.iso.org/standard/67480.html
- ISA-TR106.00.01: Procedure Automation for Continuous Process Operations – Models and Terminology; refer to: https://www.isa.org/isa106
- ISO/IEC/IEEE 24765:2017: Systems and Software Engineering – Vocabulary; refer to: www.iso.org/standard/71952.html
- The Industrial Internet of Things Volume G5: Connectivity Framework (IIC:PUB:G5:V1.0:PB:20170228), Industrial Internet Consortium; refer to: https://www.iiconsortium.org/IICF.htm

1 Introduction

1.1 Objective

The objective of Part 1 of the O-PAS Standard is to define the components that make up the O-PAS specification. This document lays out the overall Technical Architecture, developed by the Open Process Automation™ Forum, a Forum of The Open Group, of an O-PAS conformant system though a set of interfaces to the components. The detailed interface specifications are defined in the other parts of the O-PAS Standard and contain the associated conformance criteria. The objective of the Technical Architecture is to meet the requirements of a federated and secure process automation system using an open and interoperable architecture. The O-PAS Standard is defined to allow development of systems consisting of components from multiple vendors, without requiring custom integration.

Part 1 of the O-PAS Standard is informative and intended to provide a general overview of a system composed of O-PAS conformant components and to describe the general functionality of the interfaces.

The contents and security scope of the Preliminary Standard are related to the scope and overall objective of the O-PAS Standard, Version 1.0.

1.2 Overview

The Technical Architecture allows for construction of safe, reliable, secure process automation systems that are scalable from very small to very large, which do not require system shutdown to perform updates and extensions, and which can be applied to existing systems and to new construction. The Technical Architecture has been defined to not compromise the safety, resilience, reliability, maintainability, or security of a process automation system.

- To support safety and resilience, the Technical Architecture has been defined so that redundancy can be implemented on an I/O point-by-I/O point basis, reducing the scope of failure to a single loop and providing the capability for automatic transfer of control logic
- To support resiliency, the Technical Architecture has been defined so that it provides the environment for *m*-to-*n* redundancy, where a node may assume the role of a failed node and either run its applications, use alternate I/O, or simulate the failed I/O
- To support reliability and maintainability, the Technical Architecture is defined so that a system can be implemented to be incrementally upgraded and enhanced, without system shutdowns and without turning off power to the rest of the system, except for components being repaired or replaced
- To support reliability and maintainability, the Technical Architecture is defined to allow incremental upgrades by replacement of components with the same or additional functionality, without system redesign

- To support reliability and maintainability, the Technical Architecture is defined to provide the ability to move applications across control elements without modifications, allowing recovery from control element failure
- To support security, the Technical Architecture has security designed into all aspects to allow low lifetime support efforts to maintain updates and patches, and to allow secure communication between components and other systems
- To support interoperability, the Technical Architecture is defined through interface functions and information models, using existing standards where feasible and The Open Group standards, extensions, or profiles where needed
- To support process automation, control strategies on multiple levels can be easily integrated, without extensive integration services
- To support scalability, the Technical Architecture is designed such that the end user is only required to buy the capability and capacity they need
- To support existing systems, the Technical Architecture does not require replacement of existing instruments or wiring

1.3 Conformance

Part 1 of the O-PAS Standard is informative, and no conformance requirements have been defined in this part. Normative requirements and conformance criteria are defined in the other parts of the O-PAS Standard.

1.4 Normative References

The following parts of the O-PAS Standard contain provisions which, through references in this part, constitute provisions of Part 1 of the O-PAS Standard. At the time of publication, the editions indicated were valid. All parts are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the parts listed below.

- O-PAS Part 2 – Security (Informative), Preliminary Standard (P190-2), January 2019, published by The Open Group; refer to: www.opengroup.org/library/p190
- O-PAS Part 3 – Profiles, Preliminary Standard (P190-3), January 2019, published by The Open Group; refer to: www.opengroup.org/library/p190
- O-PAS Part 4 – Connectivity Framework (OCF), Preliminary Standard (P190-4), January 2019, published by The Open Group; refer to: www.opengroup.org/library/p190
- O-PAS Part 5 – System Management, Preliminary Standard (P190-5), January 2019, published by The Open Group; refer to: www.opengroup.org/library/p190

1.5 Terminology

For the purposes of the O-PAS Standard, the following terminology definitions apply:

Can	Describes a possible feature or behavior available to the user or application.
May	Describes a feature or behavior that is optional. To avoid ambiguity, the opposite of "may" is expressed as "need not", instead of "may not".
Shall	Describes a feature or behavior that is a requirement. To avoid ambiguity, do not use "must" as an alternative to "shall".
Shall not	Describes a feature or behavior that is an absolute prohibition.
Should	Describes a feature or behavior that is recommended but not required.
Will	Same meaning as "shall"; "shall" is the preferred term.

1.6 Future Directions

Future versions of the O-PAS Standard will address additional functionality such as portability, configuration management, application management, extended system management, and the hardware physical platform. At that time, Part 1 and its contents will be revised and accordingly updated.

2 Terms and Definitions

For the purposes of the O-PAS Standard, the following terms and definitions apply. Merriam-Webster's Collegiate Dictionary should be referenced for terms not defined in this section.

2.1 Terms

For the glossary of terms, see the definitions here.

3 Technical Architecture Concept Overview

Figure 1 is a concept diagram that illustrates a process automation system that is a collection of O-PAS conformant components. The conformant components are Distributed Control Nodes (DCNs) connected via the Connectivity Framework (OCF).

The OCF provides for determinism and quality of service required for data exchanges that are sufficient to support a distributed control logic execution environment. An O-PAS system is a collection of O-PAS conformant components all exchanging information using the OCF.

A DCN is defined as a combination of a Distributed Control Platform (DCP) and one or more Distributed Control Frameworks (DCFs) running applications. A component which does not have a conforming DCP (for example, Distributed Control System (DCS), Programmable Logic Controller (PLC), analyzer, etc.) may also host DCFs. The applications hosted by these DCFs communicate through the OCF interface.

Applications are single indivisible components comprised of a program and associated configuration and data that performs a set of coordinated and related functions. See Appendix B for more information on applications.

Connectivity to non-conformant O-PAS devices is provided through DCNs performing gateway functions to make the non-conformant O-PAS device's information accessible through the OCF interface.

Each component in the system may execute all or part of the overall control and operations strategies, based on the capabilities and capacities of the components.

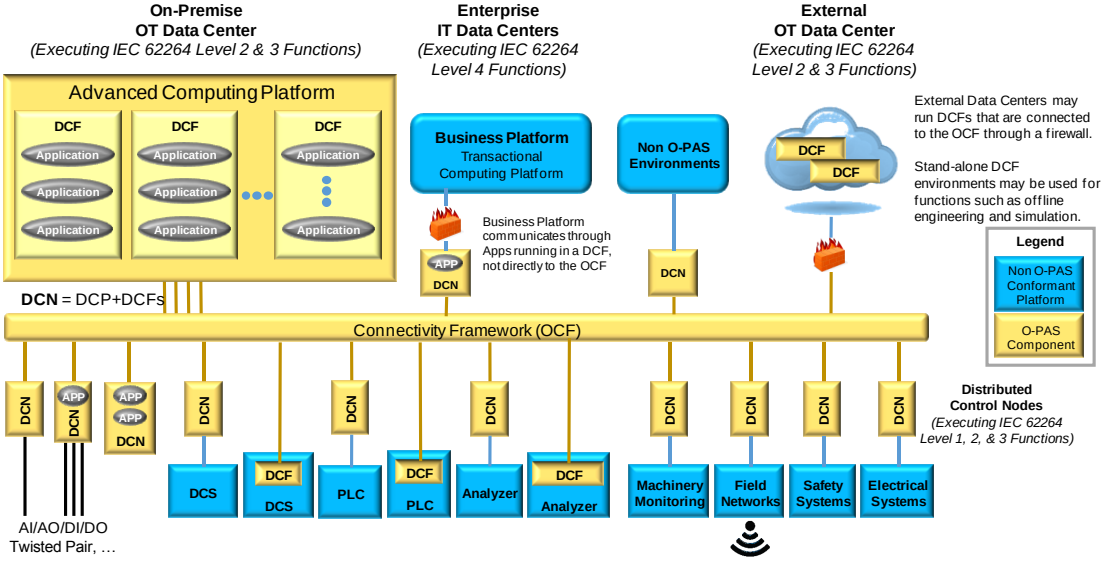

Figure 1: Concept Diagram of a Process Automation System of O-PAS Conformant Components

3.1 Connectivity Framework (OCF)

The Connectivity Framework (OCF) is a royalty-free, secure, and interoperable hardware and software communication framework specification, specified in O-PAS Part 4 – Connectivity Framework (OCF).

While the OCF is shown as a single network in Figure 1, actual implementations will usually consist of segmented networks to support security, performance, and quality of service requirements.

3.2 Distributed Control Node (DCN)

A Distributed Control Node (DCN) is a type of device that connects to the OCF.

DCN types include the following, possibly overlapping types:

- DCNs with physical I/O
- DCNs without physical I/O
- Advanced Computing Platforms (ACPs)

  An ACP is a computing platform which implements DCN functionality but has scalable computing resources (memory, disk, CPU cores) to handle applications or services that require more resources than are typically available on a small profile DCP.

  ACPs may also be used for applications which cannot be easily or efficiently distributed.

  The O-PAS Standard does not prevent additional functionality not defined in the standard from being available in an ACP.

- Gateways

  A DCN which provides OCF interoperability to a software component, device, or a system, which is not natively O-PAS conformant.

  For example, a DCN acting as a gateway may be connected to a legacy DCS, legacy PLC, smart device, Highway Addressable Remote Transducer (HART) device, Foundation Fieldbus device, or a network of such devices.

- Devices, such as DCSs, PLCs, analyzers, etc., containing one or more embedded DCFs

  Devices with embedded DCFs are visible through the OCF as if they were DCNs, even though they have different physical form factors, and they may not support interchangeability of standardized physical components.

Each DCN or embedded DCF can be configured based on the role it performs in the overall automation and operations strategies. This allows replacement of a DCN to be a simple maintenance action, with no excessive manual configuration except to specify the role of the new DCN.

3.3 Distributed Control Platform (DCP)

A Distributed Control Platform (DCP) is the hardware and system software platform of a DCN. It provides the environment for DCFs and applications as well as providing the physical

infrastructure and interchangeability capability. DCP types are defined through profiles, with different functionality specified for different platform hardware specifications.

See O-PAS Part 3 – Profiles for additional information on profiles.

3.4 Distributed Control Framework (DCF)

A Distributed Control Framework (DCF) is the environment for execution of applications through a set of interfaces.

The DCF provides an environment where applications can be moved between DCNs. It contains means to protect IP of function block types and function block instances. This is important to create an efficient marketplace for O-PAS applications.

DCF types are defined through profiles, with different functionality specified for different capabilities. See O-PAS Part 3 – Profiles for additional information on profiles.

3.5 Applications

An application is a single indivisible element comprised of a program and associated configuration and data that performs a set of coordinated and related functions. There are different types of application defined in the O-PAS Standard (see Appendix B):

- Companion Configuration Format applications

  These are specific types of platform-independent applications written using one or more of the industry standard platform-independent control languages, defined through Companion Configuration Formats (such as IEC 61131-3 or IEC 61499-1 languages). Because Companion Configuration Format applications are based on platform-independent languages, they are inherently portable to different environments.

- Platform-independent applications

  These are applications (such as an IEC 61131-3 program execution application, a Human-Machine Interface (HMI) application, or a data historian) written to run in the DCF environment using the DCF services.

- Platform-dependent applications

  These are applications written to execute using the native DCP O/S and services (such as a control application using O/S-specific functions or a HMI using native hardware features).

3.6 Equipment with Embedded DCF Functionality

The system may contain equipment with embedded DCF functionality, defined as a type of DCN in Section 3.2. This is equipment which does not conform to a DCP profile but does provide the capability of participating in OCF communication and potentially hosting applications. Devices with embedded DCFs are visible through the OCF as if they were DCNs. Possible examples are field instruments, DCSs, PLCs, analyzers, safety systems, and electrical systems.

3.7 Business Function Connectivity

The system may contain connectivity to business functions (such as Enterprise Resource Planning (ERP), Material Resource Planning (MRP), Product Lifecycle Management (PLM), Supply Chain Management (SCM), and other business systems running in IT data centers).

Connectivity to business software is through applications running in a DCN. The connection between the OCF and business networks is shown in Figure 1 connected through a firewall as an example, following the recommended best practice as documented in the ANSI/ISA 62443 standards.

3.8 External OT Data Centers

The system may support communication to external Operations Technology (OT) data centers to support applications running IEC 62264 Level 2 and Level 3 functions. In addition, OT data centers may execute functions not defined in the O-PAS Standard, such as offline engineering tools, simulation tools, and management tools.

Connection to OT external data centers is shown in Figure 1 controlled by a firewall between the OCF and the external OT data center as an example, following the recommended best practice as documented in the ANSI/ISA 62443 series. However, applications running in external OT data centers may participate directly in OCF communication, if allowed by local security rules.