ISASecure Web Conference

OPAF Cybersecurity and Testing

ISASecure®

About the Speaker

- **Camilo Gómez**
- **Global Cybersecurity Strategist**

- **Camilo Gómez** is principal technology strategist at Yokogawa's USTC subject matter expert in OT cybersecurity and risk management delivering strategic thinking within Yokogawa and the automation industry. His broad 30 years experience encompasses leading global OT cybersecurity and IT programs in support of industrial systems with exposure in O&G, industrial automation, and business consulting. Mr. Gómez currently serves as Co-Chair of the *Security Architecture subcommittee* of OPAF, and Co-Chair of WG12 the *Performance Metrics for IACS Cybersecurity* working group of ISA99. Mr. Gomez is also board member of ISCI, and senior level member of IEC TC65 WG10 and IECEE CMC WG31.

ISA Security Compliance Institute

Agenda

- What is O-PAS?
- O-PAS Vision
- O-PAS Security Framework
- Technical architecture
- How to apply IEC 62443 to O-PAS?
- O-PAS Part 2 Security
- Security testing and certification challenges
- ISICI OPAF Security Testing of O-PAS Products

ISA Security Compliance Institute

What is O-PAS™?

THE OPEN GROUP
OPEN PROCESS AUTOMATION™ FORUM

Saudi Aramco is a member engaged with the Technical Working Group developing the Standard including the Security Architecture Framework

What is O-PAS™?

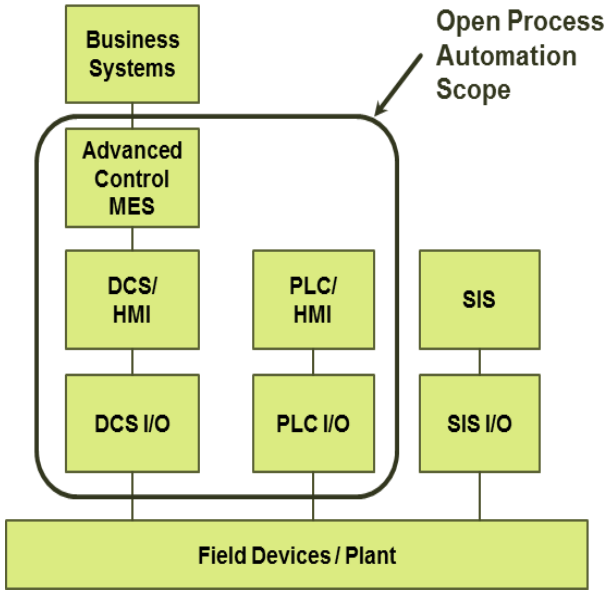
Standards based

Open

Secure

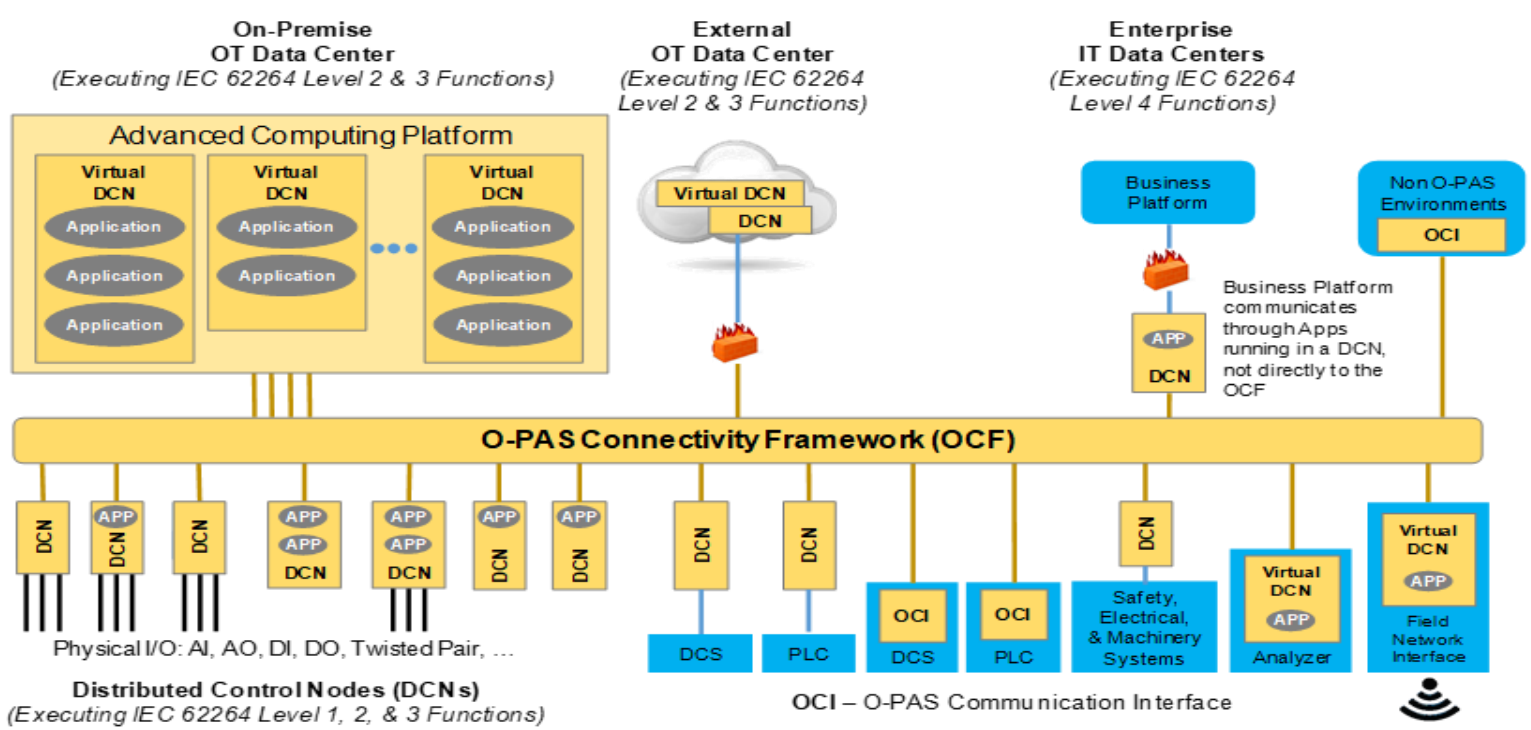
Interoperable

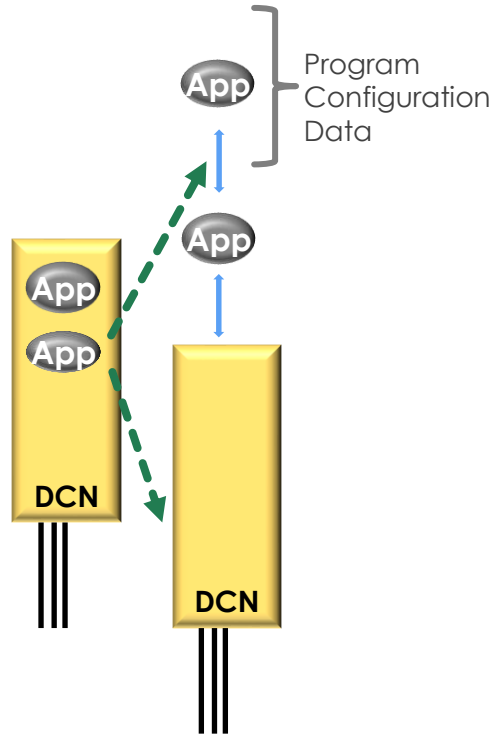
Process Control Architecture



ISA Security Compliance Institute

O-PAS™ Vision and Components





Source: The Open Group - O-PAS™ Standard - Copyright © The Open Group 2020

ISA Security Compliance Institute

O-PAS™ Challenge – Secure by Design

OPAF End-User requirements

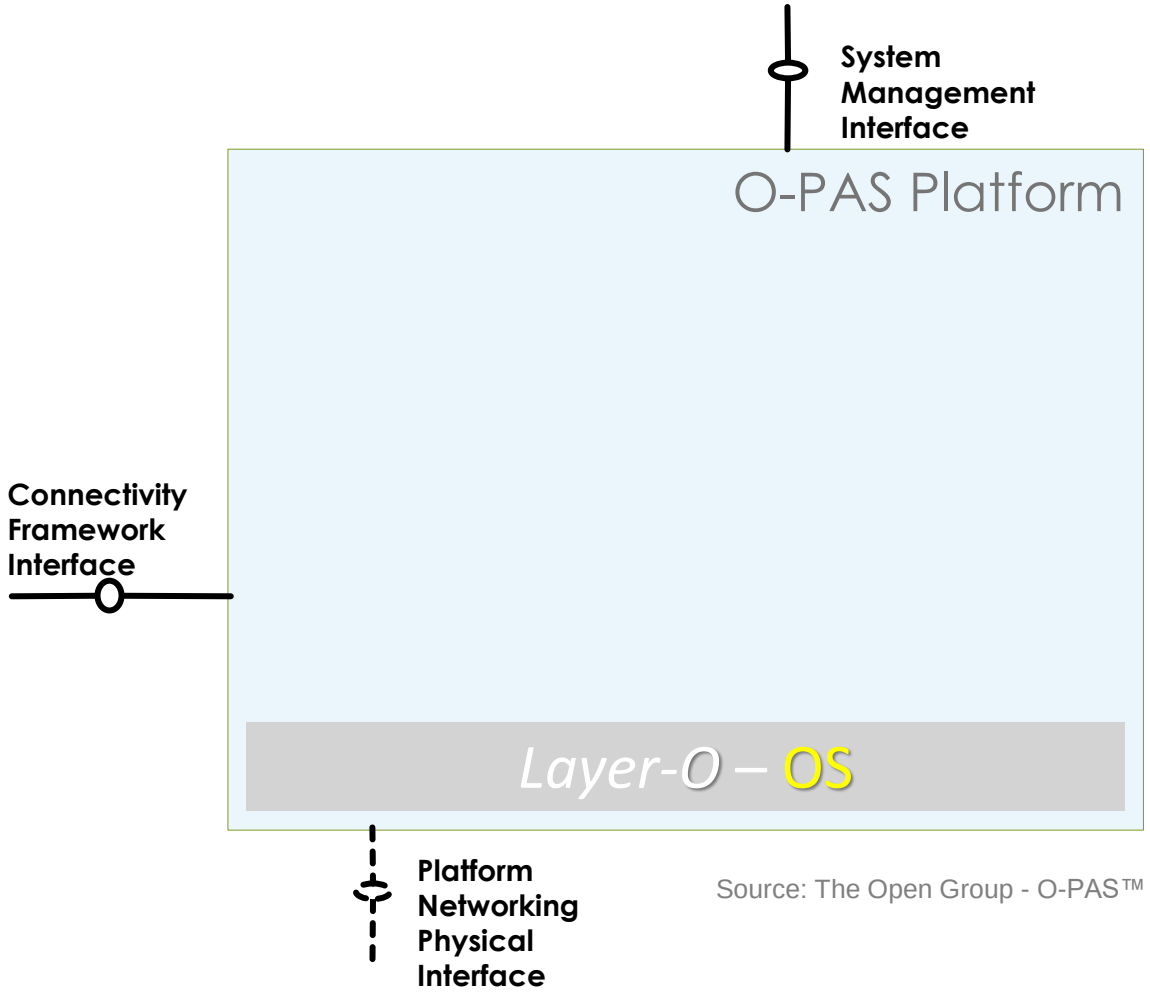
- The O-PAS architecture shall **take advantage of existing industry standards** whenever possible and practical and consistent with achieving the goals of the O-PAS Standard.
- O-PAS components shall **meet or exceed the Security Levels (SLs) defined in industry standards**, as determined by the system owner.
- The O-PAS Standard shall **allow for the development of O-PAS components using secure programming practices** and restrictions.

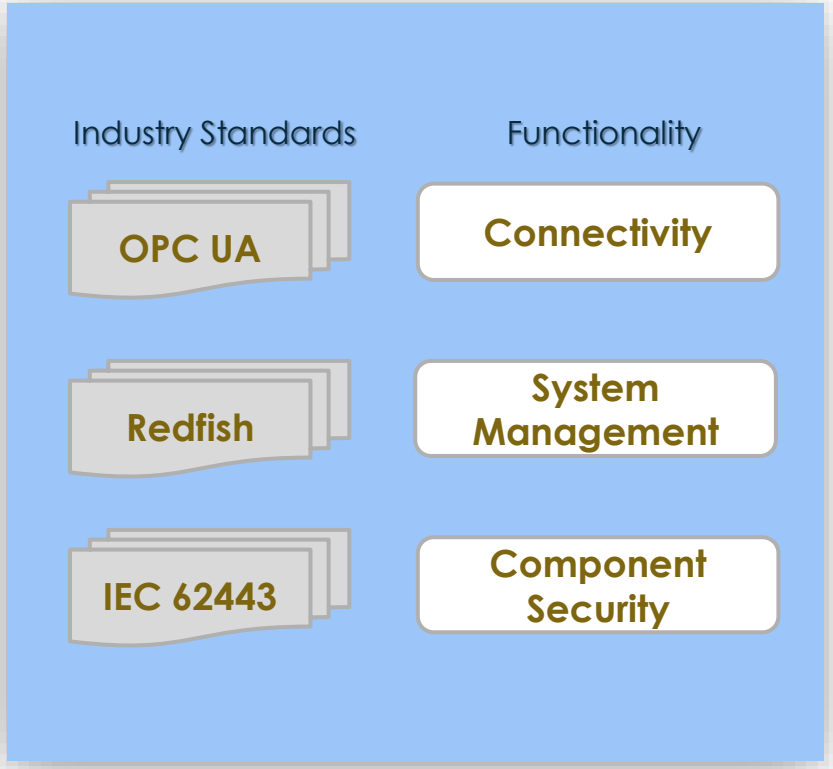
Security Framework

- IEC 62443 standards for Components
- SL2 – Security Level

ISA Security Compliance Institute

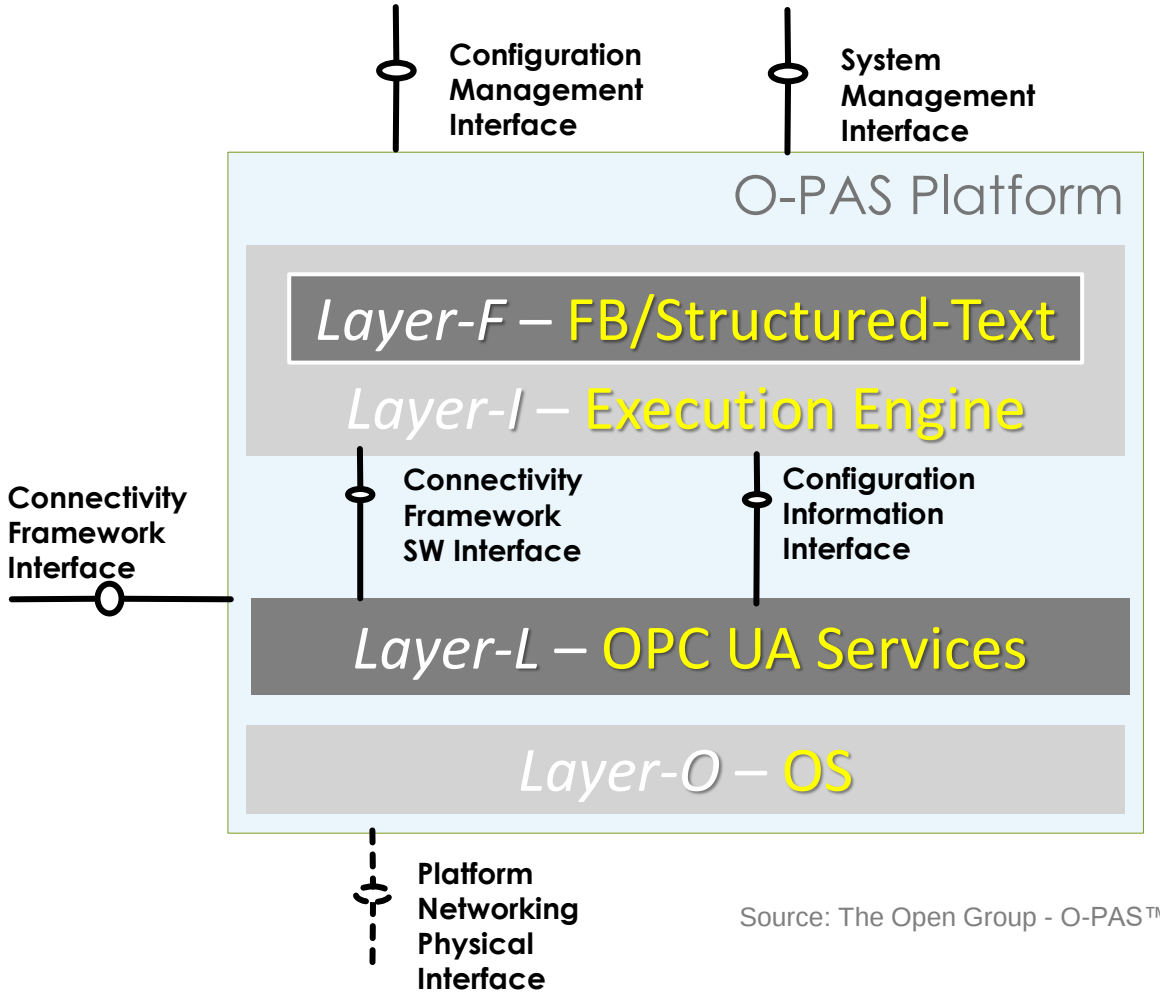
O-PAS™ V1 – Interoperability

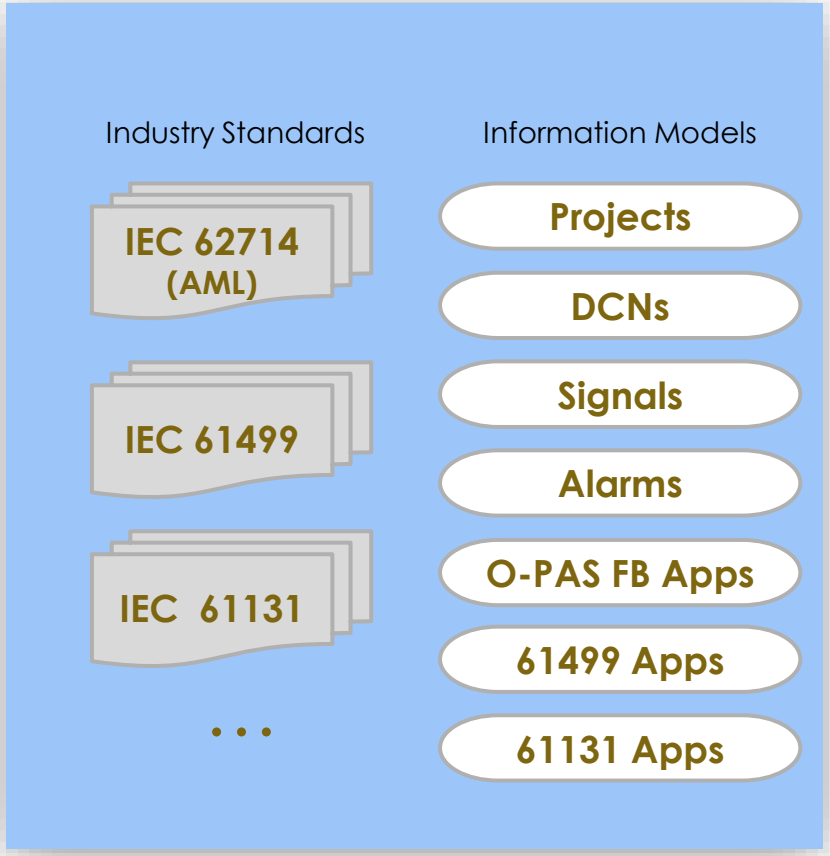




ISA Security Compliance Institute

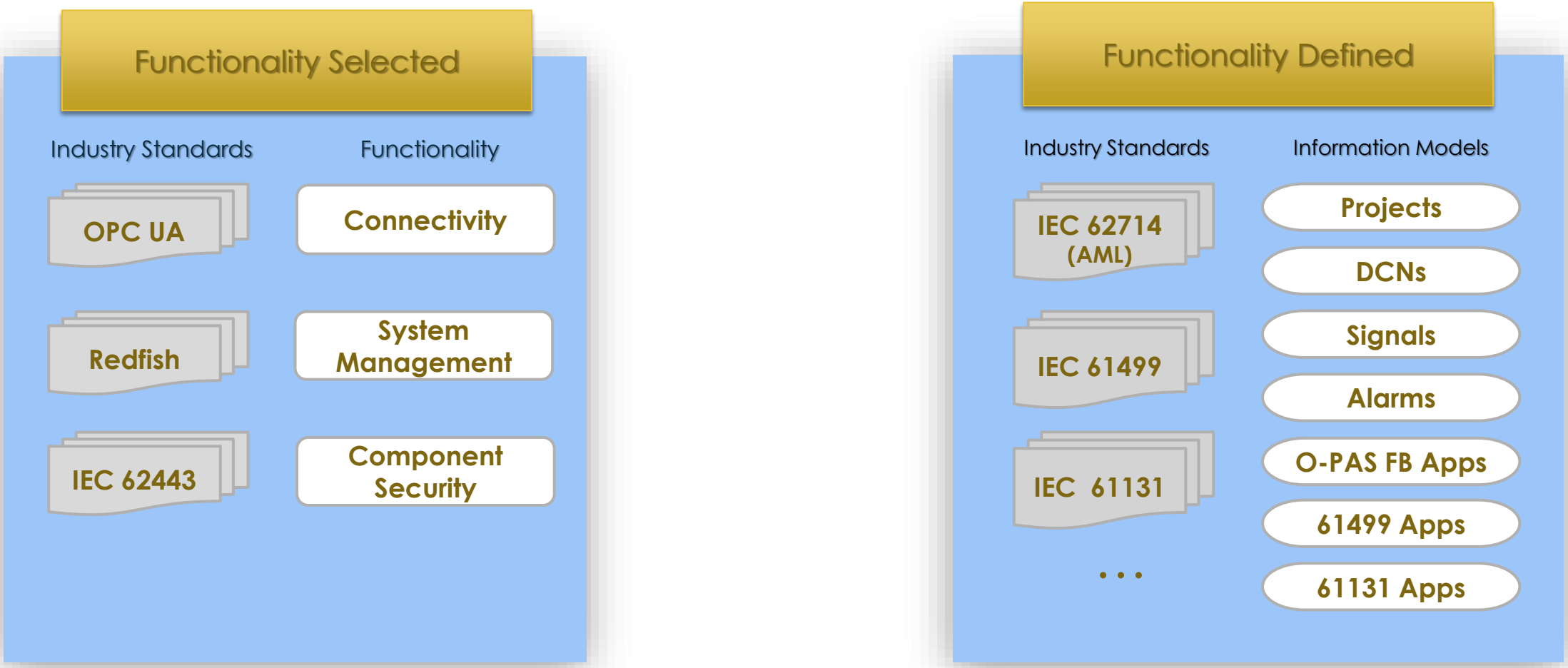
O-PAS™ V2 – Configuration Management





ISA Security Compliance Institute

How to apply IEC62443 to O-PAS™?



ISA Security Compliance Institute

O-PAS™ Part 2 Security

- *Normative*
  - Security Facet with IEC 62443-4-2 SL2 requirements applicable to O-PAS functionality
- *Informative*
  - Mapping of OPC UA to IEC 62443-4-2
  - Mapping of Redfish to IEC 62443-4-2
  - IEC 62443-4-2 security control areas relevant to Configuration Management
  - IEC 62443-4-2 security control areas relevant to Physical Platform

ISA Security Compliance Institute

Challenges to Cybersecurity test and certify

- O-PAS incremental functionality
  - Test or externally certify?
- O-PAS moving away from the device mentality
  - Are external certifications ready for O-PAS component types/products?
- External certification vs The Open Group OPAF Certification
- Learning process for both OPAF and ISCI

ISA Security Compliance Institute

ISCI and OPAF MOU

- Commitment to cooperate in a component cybersecurity assessment/testing program.
- Program implemented in accordance with relevant O-PAS™ specifications and associated certification program.
- ISASecure to assess the security conformance of O-PAS™ products using ISASecure's certification specifications derived from IEC 62443 standards.

ISA Security Compliance Institute

Summary

- O-PAS standard
- O-PAS Vision
- O-PAS Security Framework
- O-PAS Technical architecture
- O-PAS and IEC 62443
- O-PAS Part 2 Security
- OPAF Certification and ISCI security testing

ISA Security Compliance Institute

Thank you

Questions?

ISA Security Compliance Institute