OCTOBER 25, 2023

Has OPC DA finally reached end-of-life?

How to migrate to OPC DA in a heightened security landscape

Xavier Mesrobian

Xavier Mesrobian

Vice President Sales and Marketing

- Skkynet
- xavier.mesrobian@skkynet.com

Agenda

OPC DA overview

OPC UA overview

Renewed focus on Cyber Security

Shift in Architectures

Real world examples

About Skkynet

Critical Infrastructure for over 25 years

- 27,000+ installations in 86 countries
- Used by the 10 top automation providers worldwide
- OEM relationships with hardware and software providers
- Certified AVEVA Technology Partner
- Covering energy, discreet manufacturing, water/wastewater, building automation, oil & gas, and minerals & mining to name just a few

OPC DA

Understanding OPC DA

- Introduced by the OPC Foundation in August 1996
  - Underlying technology is based on Microsoft Distributed Component Object Model (DCOM)
- Today over 80% of Industrial systems still use OPC DA
- Challenges
  - Difficult to configure
  - Difficult to secure
  - Hard to maintain
- Microsoft has been hardening DCOM from its inception, as they are aware of the security risks with DCOM.
  - They discovered a vulnerability in that a potential attacker may bypass server security to attack an organization's networked device. DCOM authentication hardening - Microsoft security patch KB5004442 tries to address this.

AVEVA

OPC UA

Better security

- Introduced in July 2006
- Advantages
  - Multi-platform
  - Better security
  - No reliance on DCOM
- Adoption has been slow, yet today most systems today now support OPC UA.
- Disadvantages
  - Although security has improved, the underlying architecture still does not make it easy to secure data across the OT – IT plane

AVEVA

Renewed focus on Cyber Security

Question is not if, but when you will be compromised

- According to IBM, the average cost of a breach is $4.45M
- It is estimated that 39% of businesses have experienced either a security breach or a cyber attack.
  - Over the last 12 months we have seen Utilities, Oil and Gas, manufacturing facilities, Department of National Security, and even Health Care providers shut down
  - Governments have weighted in

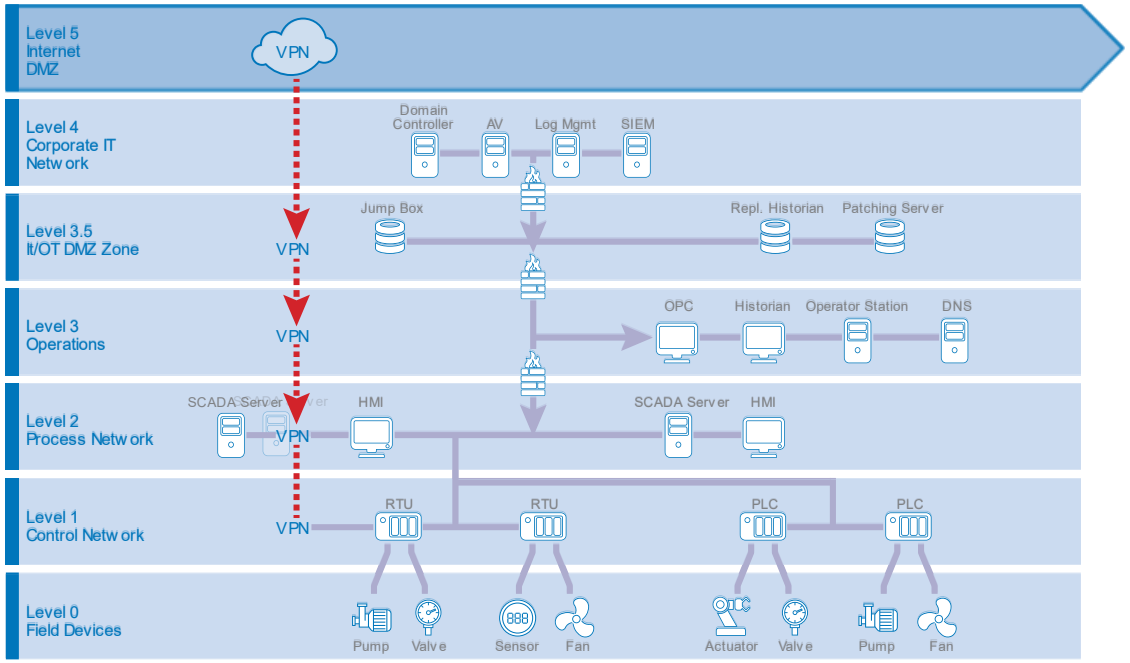
In a rare joint release both NSA and CISA recommend immediate actions to reduce exposure across operational technologies and control systems

Revised Directive on Security of Network and Information Systems (NIS2)
Key Guideline: One or more DMZs are needed for the most secure, manageable, and scalable segregation of control and corporate networks

Renewed focus on Cyber Security

Where it all starts

- Virtually all security breaches start in **IT**
- Industrial protocols were never designed for IIoT
  - Networking OPC (DA or UA) requires the client to connect to the server



Renewed focus on Cyber Security

Goal: Eliminate the attack surface on the data source

- Securing the OT network is not difficult, as long as you play by the rules.
  - It is important that data source firewalls not be open to any incoming connections
  - No open ports = no attack surface from the Internet or any adversary
  - Data source must only make outbound connection
    - Attacking outbound connections is difficult
    - SSL and strict certificate checking addresses DNS poisoning, man-in-the-middle, and packet sniffing
    - User/password/IP address authentication provides added protection
    - Authentication requires correct answers to both “Who am I?”, and “Where am I?”
- Yet, OPC DA and OPC UA require the client to open inbound firewall ports.

AVEVA

Renewed focus on cyber security

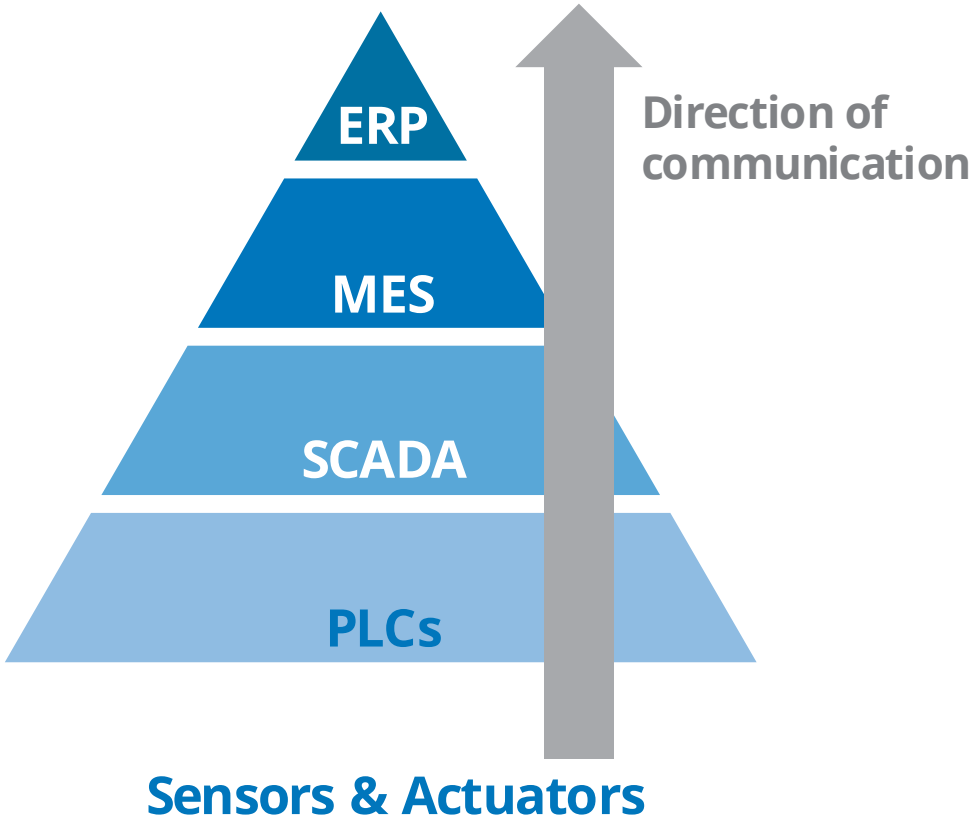
When a new solution architecture is required – Does OPC DA fit?

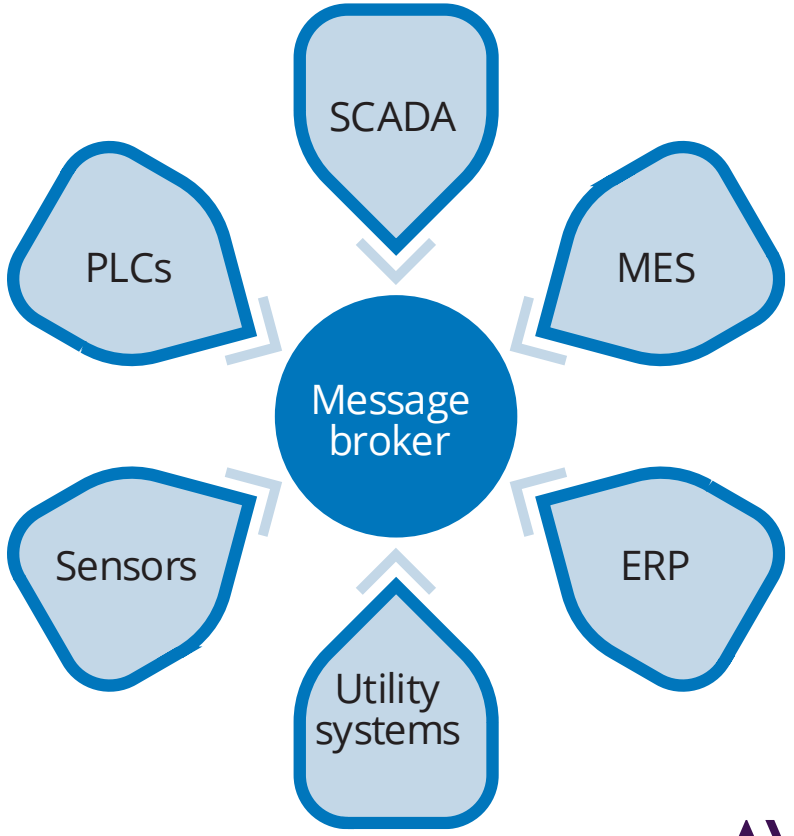
- Market Drivers
  - Analytics / AI are best implemented in the cloud
    - Cloud offers limitless storage and compute power
  - SCADA is evolving
    - First generation: Monolithic
    - Second generation: Distributed
    - Third generation: Networked
    - Fourth generation: Web-based
  - Cloud providers - AWS and Azure

AVEVA

Shifting the data sharing model

ISA 95 verses message broker architecture (sometimes referred to as UNS)

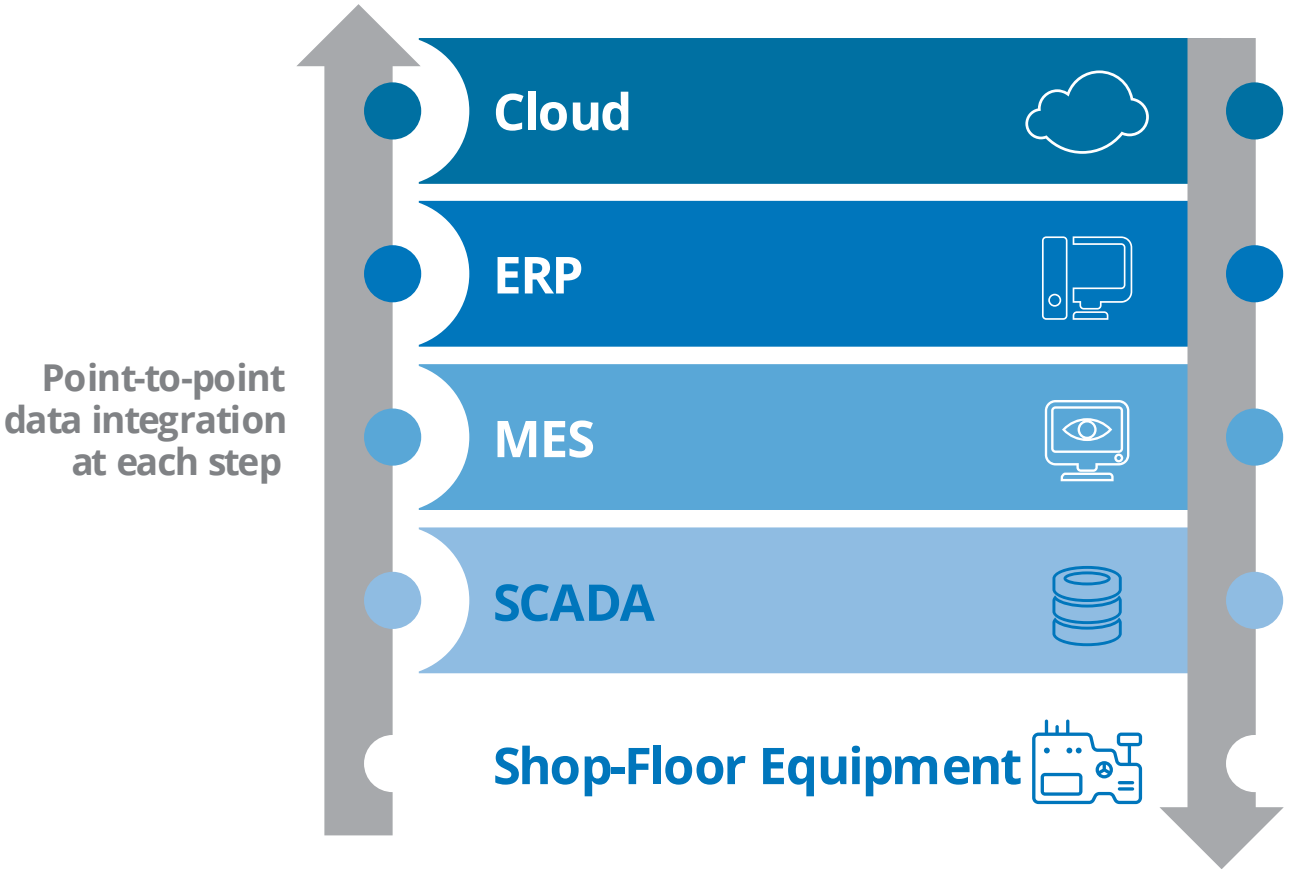




Shifting the architecture

Challenges of ISA 95

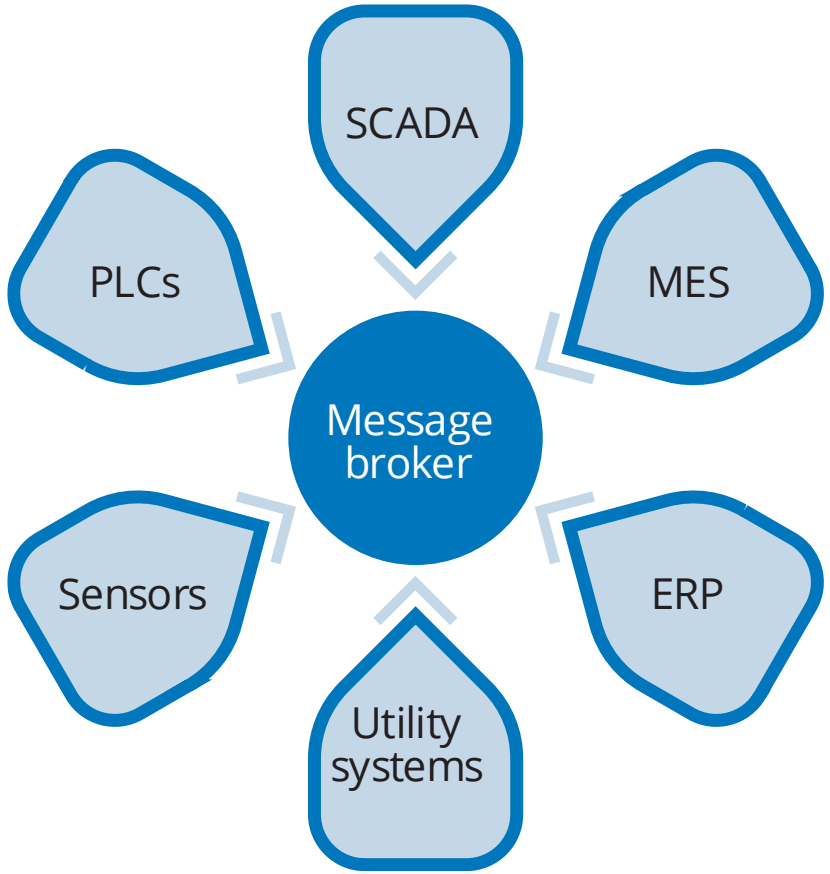
- Integration complexity
  - Point to Point data integration
- Inflexible data flow
- Requires the configuration of the same data multiple times
- Hard to combine data from multiple levels
- Moving data from multiple levels is hard to secure



Shifting the architecture

Advantages of the Message broker

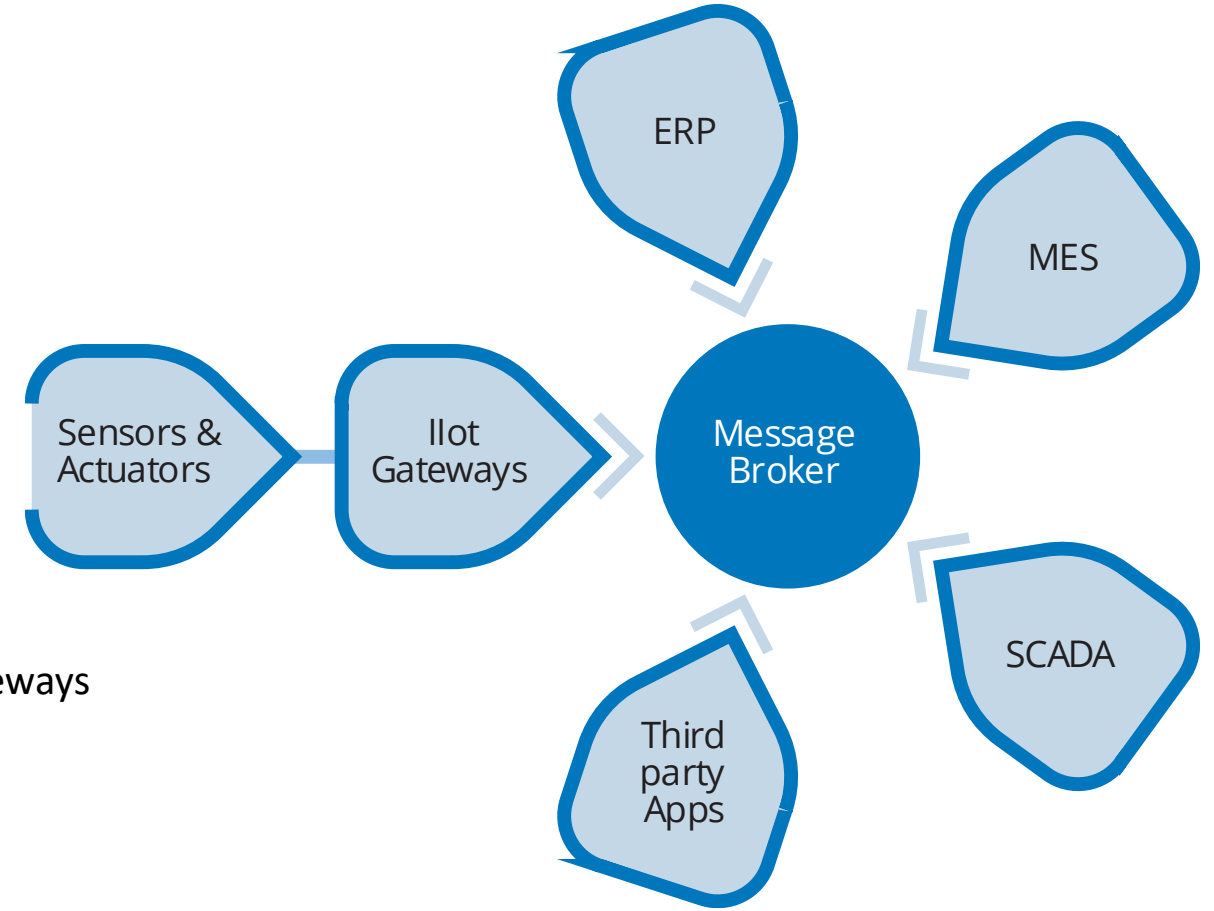
- Access to all data from all the systems
- Simplified integration
- Allows for easy application decoupling
- Simple replacement of data producers and data consumers



Shifting the architecture

Challenges in Architecture - Security

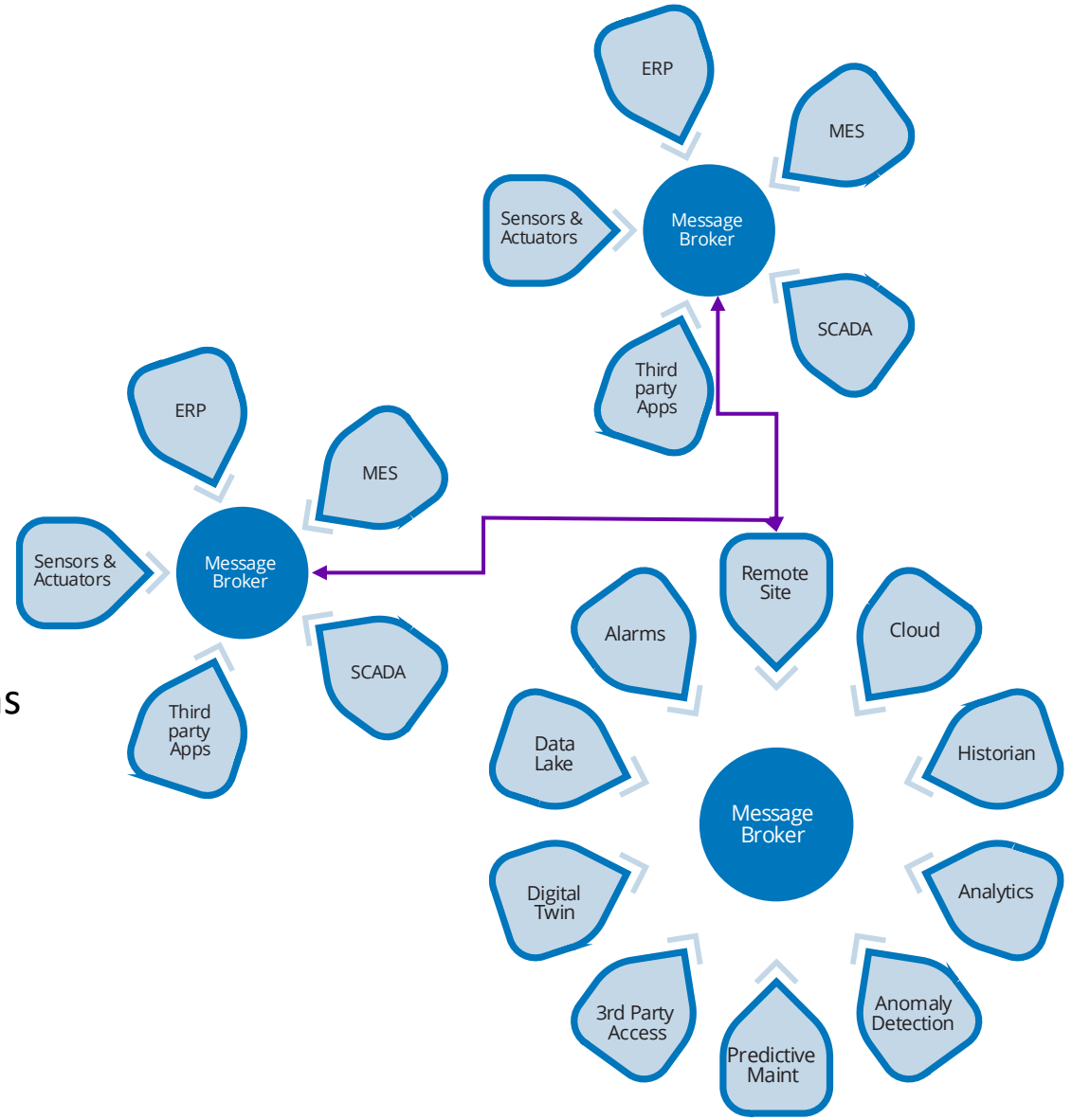
- Networking the source data can pose a challenge
  - Some data is inside your control networks
  - Some data is in your DMZ / IT network
  - Some data is going to or coming from the cloud
- Is MQTT the right choice?
  - MQTT does not guarantee message order
  - Lacks intelligent message handling
  - Daisy-chaining is fragile
  - Requires protocol translation to MQTT or the use of Gateways



Shifting the architecture

A better solution for a Message broker

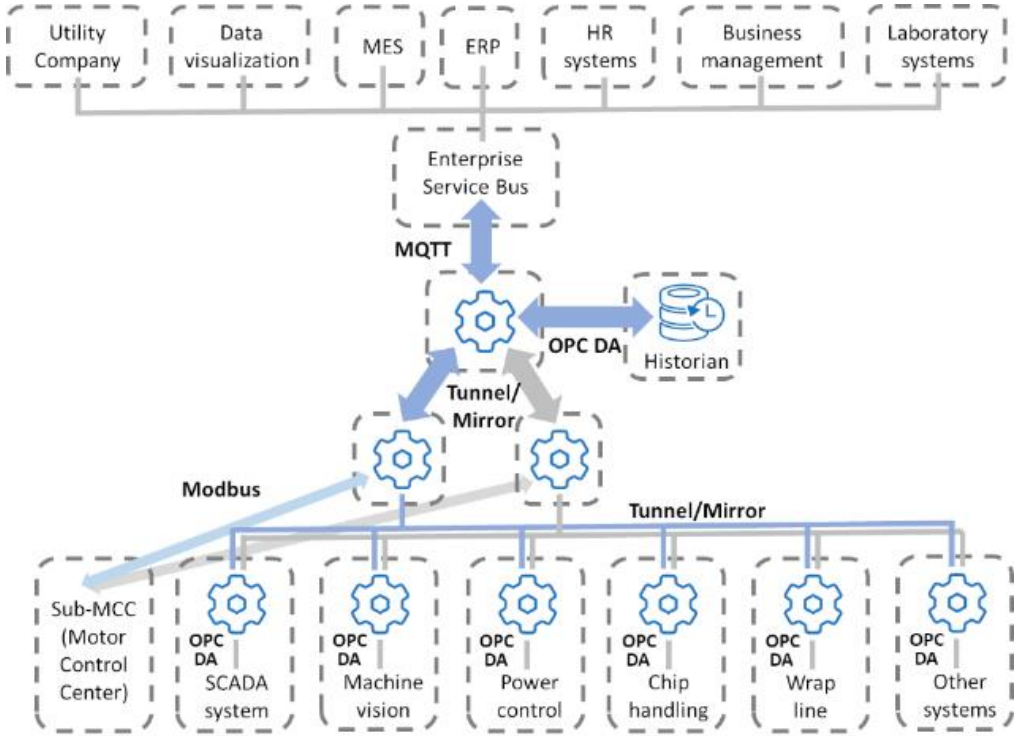
- Message broker should be protocol independent
  - Relying on one protocol means all connections must match that protocol – adds cost and complexity
- Daisy-chaining message brokers should be easy to configure, should eliminate attack surfaces, and maintain message order.
- Message Broker should support redundant communications



Real-world example with multi-protocol support

Paper industry

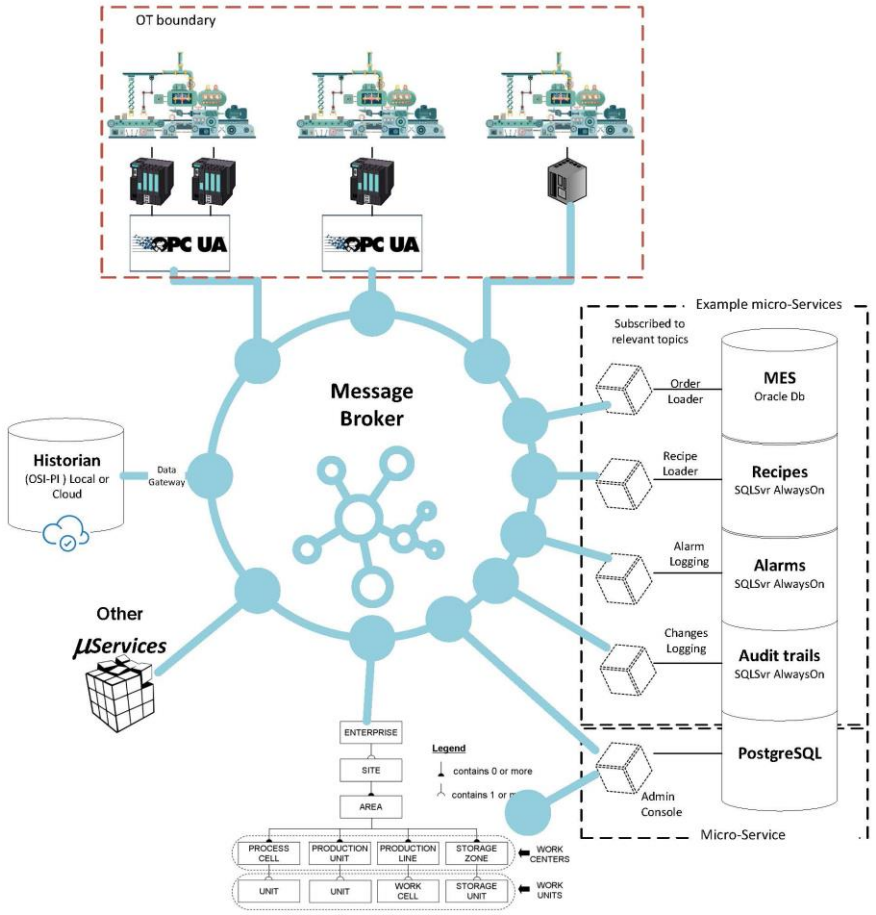
- Message broker supports multiple protocols
  - OPC DA, MQTT, Modbus TCP
  - As opposed to converting OPC DA, the client chose to Tunnel/Mirror the data – eliminating inbound firewall ports
    - Network isolation between the OT and IT networks
- Message broker resolves redundancy across the production data
  - Two redundant data paths are resolved
- Historian is connected to the message broker
- All systems have access to all data



Real-world example with multi-protocol support

Pharma

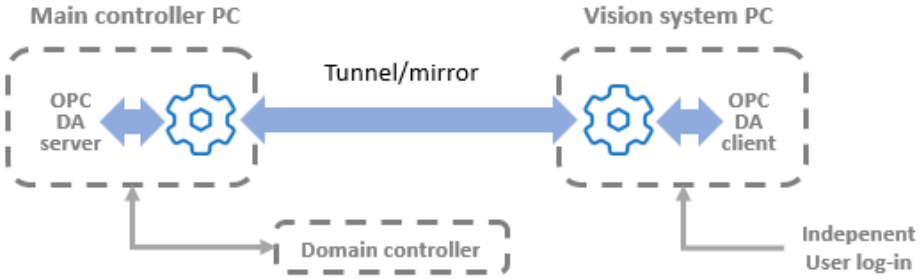
- Message broker supports multiple protocols
  - OPC UA, MQTT, ODBC
  - Here the client converted OPC DA to OPC UA.
    - They still have open inbound firewall ports, but they chose to manage that risk with layered security
- Historian is connected to the message broker
- All systems have access to all data



Real-world example DA Tunnel / Mirror

Pharmaceutical Device Manufacturing

- Implemented Microsoft DCOM hardening, but experienced connection failures
- Here the client used Tunnel / Mirror to connect DA Systems
- Keeping production running yields huge cost savings
  - Did not have to upgrade their existing software to support OPC UA



In Summary

OPC DA is not end of life

- With over 80% of existing systems supporting OPC DA and the average industrial system life span of 15 years, DA will continue to be present.
- The choice depends on your architecture and your goals
  - Implementing a message broker
    - Choose one that is protocol independent
    - Supports redundant sources
    - Designed with daisy-chaining built-in
  - Dealing with security or Microsoft hardening of DCOM
    - Conversion from OPC DA to OPC UA
      - Choose a tool that maintains the namespace instead of flattening the namespace
    - Tunnel / mirror OPC DA for added security
  - Bridging OT to IT
    - Cogent DataHub Tunnel / Mirror never opens inbound firewall ports
    - Conversion for OPC DA to MQTT

AVEVA

“We tested several products, and found the DataHub product simple, intuitive, and easy to use. When we had a challenge, it was the reaction of the people at Skkynet that impressed me. It was essentially ‘This is our problem; how do we resolve it?’ And that is something that we haven't seen before.”

Jason Burton

This presentation may include predictions, estimates, intentions, beliefs and other statements that are or may be construed as being forward-looking. While these forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could result in actual outcomes differing materially from those projected in these statements. No statement contained herein constitutes a commitment by AVEVA to perform any particular action or to deliver any particular product or product features. Readers are cautioned not to place undue reliance on these forward-looking statements, which reflect our opinions only as of the date of this presentation.

The Company shall not be obliged to disclose any revision to these forward-looking statements to reflect events or circumstances occurring after the date on which they are made or to reflect the occurrence of future events.

linkedin.com/company/aveva

@avevagroup

ABOUT AVEVA

AVEVA is a world leader in industrial software, providing engineering and operational solutions across multiple industries, including oil and gas, chemical, pharmaceutical, power and utilities, marine, renewables, and food and beverage. Our agnostic and open architecture helps organizations design, build, operate, maintain and optimize the complete lifecycle of complex industrial assets, from production plants and offshore platforms to manufactured consumer goods.

Over 20,000 enterprises in over 100 countries rely on AVEVA to help them deliver life's essentials: safe and reliable energy, food, medicines, infrastructure and more. By connecting people with trusted information and AI-enriched insights, AVEVA enables teams to engineer efficiently and optimize operations, driving growth and sustainability.

Named as one of the world's most innovative companies, AVEVA supports customers with open solutions and the expertise of more than 6,400 employees, 5,000 partners and 5,700 certified developers. The company is headquartered in Cambridge, UK.

Learn more at www.aveva.com

AVEVA